FEDERAL TRADE COMMISSION

I N D E X

FTC SPAM SUMMIT:

THE NEXT GENERATION OF THREATS AND SOLUTIONS

FEDERAL TRADE COMMISSION

601 NEW JERSEY AVENUE, N.W.

WASHINGTON, D.C.

DAY 1

WEDNESDAY, JULY 11, 2007

P R O C E E D I N G S

- - - - -

WELCOME

MS. CHRISS: Good morning, everyone. Hi there. Please take your seats, we are about to begin. This is it. Spam Summit, the Next Generation of Threats and Solutions. I am so pleased and delighted to see all of you here. This is wonderful. I see that we are going to have some very good debate, just by the faces in the audience. I recognize a lot of you from our past events. So, thank you for being here.

Before we get started, I do have a few housekeeping announcements. So, let's just get through them. If you have a cell phone, or any other noise maker, just turn it off. Just turn it off now. It is a good time to turn it off. Otherwise, there's a risk, you could receive spam from us if you don't, so turn it off. Turn it off.

The other thing is, we are a Federal Government agency and we do practice certain safety measures. If there is an emergency, and that is very unlikely, you have two exits, the way you came in, and then out through the hallway and straight back. We also practice something called shelter in place. If that happens, you will go into the hallway and wait for further

instructions.

This is the meat of the matter: You, the audience, are so integral to this, so I want to tell you the three ways you have to participate. We will have a roaming microphone at the end of each panel, so wait for the mic', state your name and your affiliation and go for it. The other way, if you're out there in webcast land, you can email us at spamsummit@ftc.gov, and you can also use your question note cards if you are in the room and they will be provided to the moderators. So, we want to hear from you.

Now, without further delay, I would like to introduce our chairman. She is a leader in this technology arena, and she has been so incredibly supportive of all of our consumer protection efforts in this area, and I'm so pleased to introduce, without further ado, Chairman Deborah Platt Majoras.

(Applause.)

OPENING REMARKS BY CHAIRMAN MAJORAS

CHAIRMAN MAJORAS: Well, thank you. Wow, we don't usually have a stage. Thank you so very much, Sana, and thanks to you and your team for all the great work putting this together. Welcome to everyone here. I'm particularly grateful to all of our very distinguished panelists for joining us for the next two

days.

In 1971, C. P. Snow, noted British author and commentator on science and technology issues, said of technology, "It brings you great gifts with one hand, and it stabs you in the back with the other." Although spam was known only as lunch meat, mystery meat, I don't know, back in 1971 when he said this, his quote is really spot-on with respect to email and spam.

Email technology has brought us great gifts in the form of quick, efficient, ubiquitous communication, but it's also brought us spam, which has the potential to metaphorically stab us in the back by inundating consumers' inboxes with unwanted email, facilitating fraud and malware and frankly betraying consumers' trust and confidence in the Internet and the electronic world.

In 2003, the FTC convened a spam forum to discuss the technical, legal and financial issues associated with spam. Now, today and tomorrow, in a continuing effort to stay apprised of developments, we want to explore the next generation of spam threats and solutions.

The volume of unsolicited emails being reported by email filtering companies is rising, creating significant cause for businesses and consumers alike. Botnets, the networks of hijacked personal computers

that spammers are using to conceal their identities, has become the preferred method for sending spam. Even more troubling, spam reaching consumers' inboxes is more often being used to launch phishing attacks and to deliver malicious code or malware to consumers' computers.

This new generation of malicious spam goes beyond mere annoyance. It can result in significant harm to consumers and undermine the stability of the Internet and of email in particular.

If you click on a link in an email message, you may be lured to a website that will either trick you into you divulging your personally identifying information, or infect your computer with spyware or other types of malware. Even merely opening a malicious email can subject you to harm. The surreptitious development of such malware can result in slow computer performance at a minimum. Installation of key logger software that can record and then report on your every key stroke. The spread of computer viruses, and the hijacking of your computer for use as a botnet.

In addition, new threats to communication media other than email are knocking on the door. Spam's cousins, spim, which is spam over instant messaging, spit, spam over Internet telephony, spam to mobile

devices threaten to undermine the benefits of mogul services and Internet telephony in the same way as spam.

Social networking websites have become yet another frontier for spam messages. The lessons we've learned and continue to learn from spam, thus, are going to be valuable as we address, or even better, try to avoid similar problems in these other communications technologies.

Now, we have to work to combat malicious spam in several ways, and the first is through law enforcement. We cannot permit the electronic frontier to become a lawless world. The FTC has engaged in aggressive law enforcement to combat spam, and since 1997, we have aggressively pursued deceptive and unfair practices perpetrated through spam in 89 law enforcement actions against 142 individuals and 99 companies, with 26 of the cases filed after Congress enacted the CAN-SPAM Act in late 2003.

For example, in one recent case, FTC versus Dugger, the FTC sought to stop the underlying use of botnets to send spam. We allege that the defendants relayed sexually explicit commercial emails through other people's home computers without their knowledge or consent, in violation of the CAN-SPAM Act, and under the final order obtained in the case, these defendants are

banned from continuing to violate the act and they are to turn over all of their ill-gotten gains.

Of course, malicious spam can also be used as a means to disseminate spyware or other malware that causes the same problems and the FTC has been actively pursuing spyware companies using our authority under Section 5 of the FTC Act, and we have brought about a dozen law enforcement actions in the past two years.

In most instances, though, the acts of malicious spammers are criminal. Criminal law enforcement agencies are best suited to expertly shut down those operations. So, for example, in June, the FBI and the Department of Justice announced a crackdown on botnets and those who control them. As part of this operation, the FBI and DOJ identified over one million personal computers infected with malware that allowed them to be hijacked and used as a part an army of bots to allow other computers to send malware and send spam.

Today the crackdown has noted three arrests: Robert Soloway who allegedly sold spam kits and botnets for spamming; James Brewer who allegedly compromised more than 10,000 PCs around the world; and Jason Downey, who allegedly ran a botnet used to conduct distributed denial of service, DDoS attacks.

So, while there's no single solution regarding

the use of botnets exclusively, these law enforcement actions are significant in this effort.

Now, a second way to defend ourselves against malicious spam is knowledge. That is knowing with whom we're interacting. Just as we can ask visitors to swipe identification badges used by metric identifiers to verify who's entering our physical space, we can use authentication technology to verify who's entering our electronic space.

At the Commission's November 2004 Email Authentication Summit, which we co-sponsored with the Department of Commerce and NIST, the commission gathered a wide spectrum of interested parties to try to find a solution to the problem of email anonymity. We had the goal then of invigorating the search for and getting some agreement on viable email authentication tools.

Since that time, domain level email authentication and the email reputation services have been adopted, at higher levels. Over 70 percent of the Fortune 100 now authenticate their outbound email, while over 25 percent of the Fortune 500 authenticate their outbound.

Trade associations like The Directing Marketing Association and the Email Sender & Provider Coalition require their members to authenticate their email. So,

we are making progress, still not enough. The Commission urges improvement in anti-spam technology and in particular continuing in domain level authentication.

This technology, we still believe, paired with reputation and accreditation systems holds great promise for preventing spammers from operating anonymously, which is something they obviously count on. So, we intend to continue working with industry to spur these efforts.

Third, to protect ourselves, we have to practice self defense. We're all consumers. Every consumer needs to learn how to spot, avoid, and defend themselves against malicious spam. We've taken many steps to educate consumers about how to avoid problems with phishing, malware and spam bots in consumer alerts, such as, should I sing this, botnets and hackers and spam, oh my, on our comprehensive educational website, Onguard Online. These educational materials encourage consumers to use anti-virus and anti-spyware software to keep their spyware up to date, among other tips.

During this summit, we are going to explore other measures that both consumers and businesses can take to further empower themselves, and on this in particular, we absolutely need your help. The biggest problem we have in consumer education is not with

pulling together the right materials, and we do get help from industry in doing that, it's distribution. Every one of us can help with that issue.

Fourth, just as we sometimes need help to protect ourselves in the physical world, collaboration among all the stakeholders in the electronic world is invaluable. Absolutely critical in this fight. Given the technical aspects of the spam problem, continued collaboration with experts from the technical community, including ISPs and email filtering companies, will strengthen these efforts against malicious spam. In addition, because of the global nature of the spam, international cooperation is essential.

Most of our enforcement actions involving spam have had international component and we've been cooperating with our law enforcement counterparts around the world in battling. We're cooperating not only on individual cases, but we're very active in the London Action Plan Initiative, which we helped start, an informal network of spam enforcers and industry representatives from over 20 countries that allow us to discuss cases, techniques, investigations, educational initiatives and the like.

Of course, the recently enacted U.S. Safe Web Act, which gives us authority to cooperate even more

closely with our overseas counterparts, gives us the tools we need to strengthen that program and we are using those to cooperate today.

Now, my hope is at this two-day summit, you all will work with us to further explore this problem and the approaches I have just outlined and new approaches. By the end of the summit, we would like to have a record that defines the malicious spam problem, identifies methods used for sending this spam, uncovers the malware economy, how they're making money, identifies threats that malicious spam posts to emerging platforms like mobile device and social networking websites, examine the methods that law enforcement can deploy to deter these malicious spammers and cybercriminals, develop new education for putting consumers back in control, explore technological tools for keeping malicious spam out of the inboxes, identify best practices for legitimate email marketers, and finally, establish a plan that we can quickly implement as the stakeholders here to reduce the deleterious effects of spam bots and malicious spam.

The risk that malicious spam will erode confidence in the Internet benefits to consumers is too great to ignore, and we have to continue to act quickly to try to address it. As my former colleague, Commissioner Orson Swindle said at our last spam forum

in 2003, we all have to work together to address this problem, and that's why we're here today.

So, I look forward to the continued development and collaborative initiatives as between law enforcement, international bodies, private industry, all interested groups, to combat the proliferation of spam bots and the spread of malware via spam.

So, with that, let's get down to it. I thank you all again very much for being here and we look forward to hearing from you. Thanks so much.

(Applause.)

DEFINING THE PROBLEM

MR. HUSEMAN: I would like to welcome everyone here today and it's good to see so many familiar faces from the 2003 FTC Spam Forum. As Chairman Majoras mentioned, much has changed in the world of spam in the last four years and one thing we definitely want to change in this Spam Summit from the 2003 spam forum is that we are not going to have any fights this year.

This opening panel is going to explore some of the big picture issues that we are going to discuss in more depth over the next two days, and in this panel in particular we're going to focus on defining the problem and trying to address a few key questions.

Now, the first question is that the earlier findings indicated that most spam was fraudulent, deceptive and offensive, so how has the nature of spam shifted now? The second question is, is spam now being used for malicious and criminal purposes.

Finally, we're going to try to address, is this spam reaching consumers' inboxes or is it being filtered by some of the Internet service providers filtering software and other mechanisms.

So, let me first introduce the panelists, then the panelists are going to give some brief presentations, and then I will follow that up with

questions and we will open it up to questions from the audience.

So, just starting to my left, first is Susannah Fox, she's the associate director for the Pew Internet and American Life Project, and that is a research organization that's funded by the Pew Charitable Trust to examine the social impact of the Internet.

Next is Thomas Grasso who is a supervisory special agent at the Federal Bureau of Investigation, the FBI, and Tom is continuing the work that he started in 2003 to develop the National Cyber Forensics and Training Alliance, which is a joint partnership between law enforcement, academia and industry.

Next is Trevor Hughes, who is the executive director of the Email Sender & Provider Coalition, which is a group that's trying to create solutions to the continued proliferation of spam, and ESPC's membership provides volume mail delivery services to an estimated 250,000 clients.

We start off, when I introduce my next panelist with the first audience quiz, what do Ben Affleck, rapper Eminem and Scott Richter have in common? And the answer is that in 2003, they all made Details Magazine's top ten list of the most influential and powerful men under 38. So, we won't ask Scott whether he's under 38

in 2007, but he is chief executive officer of Media Breakaway, and he founded his first online marketing company in 2001.

Finally we have Charles Stiles, who is the chairman of the Messaging Anti-Abuse Working Group, and he served on the organization's board of directors for the last three years.

So, that ends the introductions, I will start off with Susannah.

MS. FOX: Good morning. Thank you very much for having me this morning. My name again is Susannah Fox, and I work for the Pew Internet and American Life Project. We study the social impact of the Internet, which means we study who's online and what they do, but also who's not online, and why. Most of our research is based on telephone surveys, which we feel provide a pretty accurate picture of the changing population. All of our reports and our data sets are available for free on our website at PewInternet.org.

Our most recent survey report about spam found that email use has not decreased over the years, but people trust it less. Fifty-five percent of email users say that spam has made them less trusting of email, in general, which is about the same percentage as what we found in previous years. When asked if the volume of

spam in their inboxes had changed, most users say they don't perceive a change, but 37 percent of email users say that their personal email inboxes have received more spam. That's up 13 points since 2004.

Thirty-six percent of email users say they have received unsolicited email requesting personal financial information, such as a bank account number or Social Security number. That's essentially the same percentage as we found in January 2005. However, most email users describe spam as an annoyance. Only one in five email users say that spam is a big problem for them. That's a drop from our surveys three years ago.

This drop might be due to a perceived decrease in the volume of the most offensive kind of spam containing explicit adult content. Fifty-two percent of email users report having received a pornographic spam in our most recent survey, which was fielded in February 2007, down from 63 percent two years ago and 71 percent three years ago.

People are also becoming more knowledgeable about spam. They know better how to recognize it and handle it, and that seems to give them a sense of control. Sixty-eight percent of email users say they almost never unintentionally open an email message without realizing it was spam. Seventy-one percent of

email users say the use filters provided by their email provider or employers, up from 65 percent two years ago, and we also see that reflected in the data, where work email is being protected much better than personal email.

It might also be that for many people, spam has become like traffic, or even air pollution. You can complain about it, you can plan for it, you can try to avoid it, but it might just be a fact of modern life that we have to live with. Those of us who are online every day are often surprised when our survey data comes back that most people don't spend all day online. Most people don't know a lot about the technology they use, but they do rely on email and the Internet to stay in touch with family and friends and to get work done.

A majority of Internet users is not sophisticated about technology. They don't know they should upgrade to a better email provider. They don't know they should read the fine print when they sign up for a newsletter or buy a product from a new site. They do know that spam is cluttering their inboxes. The consequence of all this is a loss of trust in email.

MR. HUSEMAN: Thank you very much, and we will ask you some questions about your findings in a little bit. Over to Tom, please.

MR. GRASSO: Thank you, it's good to see everyone. My name is Tom Grasso, I am a special agent with the FBI. I work at a nonprofit entity in Pittsburgh called the national cyber forensic training alliance, which is a very unique operation, I think it's the only one of its kind right now. I am one of ten FBI staff that's assigned there, seven of us are agents, and I go to work every day where I work with people that aren't FBI, I work with people from industry, from other government agencies, from academia, and what we try to do is get the information that we need from people that are out there basically running the Internet, the ISPs, the software companies, have them share the information with us about who's attacking them, who's causing them problems, and where the crimes are occurring on the Internet. Certainly, spam is one of those major problems.

In 2003, we started up a project at the FBI CFPA called Slam Spam, and it was our intent, our goal to coalesce and bring together information from our various industry partners and get that into the hands of government and law enforcement so that we could go out and do something about the spam problem from an enforcement perspective.

I'm very happy to be here at the FTC. The FTC

has been the leader in this front as far as I'm concerned with their aggressive actions that they've taken against the various spammers and stuff like that. So, it's an honor for me to be here and also to have worked with the various investigators and attorneys for the FTC.

So, when we started this project in 2003, it was really us going out to the people in industry, many of the people that are in this room, and saying to you, what is the spam problem? What is the nature of it, and what can we do about it? And what we found out is that spam is really more than just these annoying messages that you get in your inbox. Yeah, certainly that is a big part of it, and it's something that we find most offensive about it, but really with spam, it involves all sorts of other criminal activity.

Bot networks, which are networks of thousands of and these days hundreds of thousands of compromised computers that are being used to disseminate the spam. Denial of service attacks that are occurring on a regular basis against sites that help us filter spam. The products that are often being spammertized, if you will, are fraudulent in nature, or have some type of criminal aspect to them.

So, there is a lot of bad stuff that goes on

with spam, and I think it's a worthy target of anybody in law enforcement, when you're on the Federal level or not, I think it's something that is causing a big problem on the Internet, and I think we need to do something about it, and the way that's going to happen is with collaboration, government, industry, all of us working together on this problem, and I think that this meeting that I'm here at today is a great example of that. I think we are going to help with that a lot. Thank you.

MR. HUSEMAN: Thank you very much. Now I would like Trevor Hughes to come up, please.

MR. HUGHES: Good morning. I do have some slides. Do you know how to get my slides up? There it is. Excellent.

Good morning, it's delightful to be here, my name is Trevor Hughes, I'm the executive director of the Email Sender & Provider Coalition. We are a trade association made up of companies that are trying to do the right thing in the email space. They are trying to use email legitimately in the marketplace, for good purposes, for marketplace purposes, and for a long time now we have been trying to stabilize and make more predictable the environment in which they operate.

We came into the debate, the discussion of spam

with a very clear agenda, very clear purpose, and that was that in our energy, in our enthusiasm to fight spam, we were missing one part, and that was that we needed to defend the legitimate use of this channel, which is the killer ap that we're all trying to protect in the end.

And so the ESPC has now for five years been working very aggressively to try and protect this killer ap, email, this thing that we all know and love so much. I would like to suggest that email has perhaps become one of the most fundamental tools for us in communicating in both our work and personal lives. Certainly we've seen surveys that suggest it's more important than phones and mail and other things, and I know from my personal experience and I'm sure many of you do, that you're already getting itchy to get on the hallway and get in your BlackBerry and see what's in your inbox.

Email is one of our fundamental means of communication, and we need to make sure that as we fight spam, which is a threat to the eco system of email, we also work to protect this very thing that we know and love so much.

So, what I want to talk to you about today is a little bit about what we have seen over the past four years since the last time we gathered for an event

looking at spam itself. Obviously we met in the interim to talk about email authentication. I want to talk to you about the CAN-SPAM Act and the effect that that's had on the legitimate marketplace. I want to talk to you about technology and consumer choice and consumer research that our organization conducted.

You'll hear more about that later through this event from Dave Lewis, chairman of one of our committees, and I want to talk to you about the evolution of industry practices and the differentiation between the legitimate use of email today and spam. I think we are much better today at distinguishing between those things.

I, too, like Brian, though, have to reflect, before I dive into my few slides here, on what a difference four years makes. Four years ago, the tension in this room was palpable. There was, almost, a fist fight four years ago. There were rumors that there may be people taken out in handcuffs. It didn't happen. But we were all sort of on the edge of our seats in this moment of fighting spam. I think we are all more mature, and have been around a lot longer in the debate. It's more sanguine, more professional.

I see a lot of familiar faces now, people who have been fighting this good fight for a long time. I

think that reflects upon perhaps what Susannah has said, that the problem has matured in the marketplace. Not only consumers, but the people fighting the problem have been finding things that work and working those solutions, working on new challenges, and we have just a different perception and a different focus today.

I would like to suggest that our organization really is interested in trust, and if you look at some of the business school research on what is trust in the business marketplace, it's made up of a few things, but two of the four components are competence and consistency. Certainly when I look at the ESPC, I think that we have focused aggressively on making sure that our members are competent in complying with the law, in complying with our best practices, in complying with technological solutions in the marketplace, and they are consistent in doing those things.

That's going to be my big close at the end, that I think those are two of the functions that are most different between the legitimate marketplace today and spammers, that we are competent and consistent today.

Let me speak quickly about CAN-SPAM. I know that we can probably spend two days talking about whether CAN-SPAM is a success or a failure, whether it's done anything or not done anything. I would like to

suggest to you that I think CAN-SPAM has done as much as it could, and that it is being used for the tool that it is. None of us ever should have, and if any of you ever did look at it as being a silver bullet to stop spam, you were misguided at the outset.

The CAN-SPAM Act provides a stable platform of predictable and consistent platform for legitimate businesses to engage in commerce through the channel of email. For that purpose, and for that purpose alone, I would say it has been a great success. But it also gives the FTC, and you've heard the chairman speak before, the ability to go after spammers. It gives AGs the ability to go after spammers.

I think that we have not seen the deterrent effect that we had hoped to see with the CAN-SPAM Act, that there are still fraudsters and crooks out there, many of them have moved to off-shore, phishing is still a problem, but at the end of the day, the effect on the legitimate marketplace has been great. In fact, the FTC's report to Congress suggested that something like 90-plus percent of the mainstream marketplace was complying with the CAN-SPAM Act. So, it has had an effect, and that effect has been sizeable and substantial, particularly in the legitimate marketplace.

I also want to talk about technology, and

consumer choice. We did consumer research earlier this year, and our survey showed while consumers may not be reading terms and conditions when they sign up, while they may not understand that there are better alternatives out there in terms of filtering email or moving to other email clients that may be doing a better job, they are tyrannical editors of their inbox. They know how to manage their inbox.

We all know this, in an incredibly sophisticated way. They spend a split second analyzing every single message in their inbox to determine whether they will keep it or not, and in fact, our surveys showed that they look at only two things, they don't open most messages, they look at the from line and the subject line, and if your message looks spammy or phishy or just bad from the from line or the subject line, if they don't know and trust you, if you haven't been competent and consistent in sending your message, they will delete you immediately. You never even get opened or seen.

That suggests to me that we need to perhaps move away from a paternalistic view of consumers and recognize that consumers can be an ally. They can be mobilized to help us in this fight. Certainly there are some solutions in the marketplace that are trying to do that, I think we can certainly do more.

One of the things that we certainly saw in our survey was that consumers want more buttons, not less. Many of the major email clients, web mail providers, ISPs, offer a report-a-spam button and that's it. Unfortunately, that turns out to be a fairly clumsy tool for a lot of consumers, because they know that there are some messages that they just want a safe and verified unsubscribe from. They have asked for it once, and it's not really spam, but the only tool that they have to say get me out of this email chain is to report it as spam.

Well, that has effects for legitimate businesses in their reputations in email channel, and it creates consequences in the email channel that are not good in our broader fight against spam.

So, one of the messages that we would like to convey today for sure is that I think we need to mobilize consumers and give them more tools in the inbox, allow them to report something as spam, to report something as fraud, to unsubscribe from a message, or just to send feedback to the sender. Those types of tools would be embraced, based on the research that we have.

I would also like to talk about the effective industry practices. The chairman mentioned before that we were the first organization to require our members to

authenticate email. In fact, we were one of the organizations that was at the center of developing some of the very earliest email authentication standards. We've gone beyond the CAN-SPAM Act, we've gone way, way beyond the CAN-SPAM Act. Before the CAN-SPAM Act was passed, we were requiring our members to only engage in permission-based, consent-based marketing practices, and we stand strongly by that. We think that that mix of the CAN-SPAM Act with best practices for industry that extend further is a good mix for legitimate businesses.

We've also issued standards and recommendations on deliverability, and we have conversations every week with our members. In fact, we have at least a couple of calls every week, talking about the latest technological developments and the latest deliverability challenges that exist for legitimate businesses in the marketplace.

I think that one of the things that we've seen in authentication, though, is that more senders do need to be authenticating. Our organization is significant and influential I think in this regard, but there are so many more senders. In fact, one of the problems that we have, it's sort of a chicken and an egg problem, is that senders don't want to authenticate until there's consequences on deliverability on the receiving side of the equation. So, you don't want to authenticate if

it's not going to have any effect on your mail whatsoever.

So, we need more ISPs to more consistently adopt and engage in authentication. There's some good news there, but I think there's better news that we could hope for and expect some time down the road.

I think at the end of the day, we need to realize, and this first panel is about redefining the problem, we are at a new environment, we are in a new form of communication about these issues, and the problem is not the problem that it was four years ago. The problem of spam today, the differentiation between spam and legitimate mail is pretty clear. Legitimate senders are competent and consistent. They comply with CAN-SPAM. They follow industry best practices. They authenticate their mail.

Spammers still do the kind of herbal Viagra stuff that we all know and love from four years ago, but it's become a bit more insidious today with phishing and other attacks. They are not consistent, and they're not competent, either. Sometimes they don't even spell well.

We need to recognize those inconsistencies, those incompetencies, and to differentiate between spam and legitimate mail so that we can really attack the bad

stuff and protect the good stuff.

So, in closing, I think that we can now better identify what is bad, and perhaps consumers are doing it as well as we are, and Susannah's data suggesting that consumers have a more sanguine attitude towards spam is indicative of this. We can recognize spam much better today than we ever could before. The legitimate marketplace is competent and consistent and spammers are not. I think we need to keep focusing on that differentiation, so that we can build higher walls and greater protections against these problems.

That's all I had. This is how you can get in touch with us. Thank you very much.

MR. HUSEMAN: Thank you, Trevor.

(Applause.)

MR. HUSEMAN: Now, Scott Richter, can you please come up.

MR. RICHTER: Good morning. My name is Scott Richter and I'm the CEO of mediabreakaway.com, and today I want to talk about the challenges facing legit email marketers.

What I want to discuss is unsolicited email messages, or excuse me, email versus legitimate marketing messages. There's three big challenges facing email marketers today. The first is deliverability, the

second is suppression lists and the third is consumer education.

First I would like to address deliverability. The email marketers can follow all the rules and still be blocked. There are several reasons for this. One is a lot of filtering systems are automated. This causes millions of legit messages from mom-and-pops to high-volume email marketers to be blocked.

Next, the next issue has been suppression lists, which came from the CAN-SPAM Act. At the time it was a great idea, but now many of these lists have grown to over ten million plus names on them. A lot of smaller senders who have small lists from their newsletters who put advertisements into them to earn a living do not have any way to run a list of this size against their list of maybe 100 to 500 to 1,000 users.

Lastly, I would like to talk about consumer education. A lot of times, consumers identify messages as spam that they do not, in fact, opt into and confirm their email address lists. A lot of times, the longer someone has had the same email address, the harder it is for them to remember what they have signed up for over the years.

Another issue with the consumer education is that many times they do not read the privacy policies of

the sites they are joining. A lot of times they may not be aware of what they are signing up for on the sites.

In summary, filtering often blocks legit email. Whether it's non-permission or especially on permission given email just because people don't recognize it. Ever-growing suppression lists are becoming very difficult to manage, and consumers need to be educated to not identify permission email that they have signed up for in the past as spam, as a lot of ISPs have made it more easy to identify any messages in their spam filter as spam.

That's it. Thank you.

(Applause.)

MR. HUSEMAN: Thank you, Scott. Okay, Charles Stiles now.

MR. STILES: Good morning. I recognize so many of you here this morning. You may know me as postmaster@aol, but I am speaking today on behalf of MAAWG as chairman of the board. If you're not familiar with MAAWG, it's an organization of just over 100 companies that are working together to collaboratively fight messaging abuse in all of its various forms, through best practices and white papers, reports, and serving on forums like this, providing information to those that are helping to develop solutions.

MAAWG was formed in 2004, and we have a close affiliation with a number of organizations, including the JEAG, the ESPC, which is represented here on the panel today, the Anti-Phishing Working Group, the London Action Plan, and we continue to work collaboratively, and also to develop and work on technologies, and to work with public policy, not as a lobbying organization, but as a resource to those that are helping to make decisions and helping us to combat this problem.

Where are we today that we weren't in 2004? Well, I think our mailboxes are probably a lot better off. Our metrics report shows that more consumers are using email, and that we're actually delivering the mail that we should be delivering, while we still block 75 to 80 percent of the mail every day that's coming in.

What's needed right now is a little bit of time, a little more collaboration, and we will continue to work collaboratively to come up with these solutions and will implement them as industry leaders to fight the problem. That is all.

MR. HUSEMAN: Thank you. Let's start off talking about the volume issue of spam, and what's actually reaching consumers' inboxes. Susannah, Pew had some statistics that said that consumers believe that they're actually receiving more spam in their inboxes,

but yet at the same time, it's become less of a problem and less of a nuisance. At the 2003 Spam Forum, a big point of discussion was that email was at the tipping point, where we were on the verge of consumers not being able to use email as a tool of communication in commerce, that doesn't seem to be the case now. I would like to ask the panelists what's changed and what are consumers actually experiencing today?

MS. FOX: Well, I'll start. The fears were misplaced, luckily. Everyone loves email, it's something that we see popular at every age level. We do surveys down to age 12, and up to our oldest citizens. We love our oldest citizens, because they're often home answering the phone for our telephone surveys, and it's one of the first activities that someone does online, and they continue it. Even teenagers who say that email is mostly for communicating with old people, they still use it.

MR. HUSEMAN: What do the panelists think? What is actually the consumers' inbox experience today?

MR. STILES: I think the consumers' inboxes today are already benefitting through some of the work that has been done through the government organizations, through the collaboration in the industry, through some of the technology that's been created, developed and

deployed. Consumers today are getting spam, but I think had we not put forth the effort that we've done, it would be unbearable, and right now we would be dealing with catastrophe.

MR. HUGHES: Our survey earlier this year suggested that consumers are seeing an amount, whether it's more or less, I certainly do believe that there's more spam being sent. I think organizations like AOL and Charles' good work are helping to block a lot of that before it gets to the inbox.

I think consumers, though, are also becoming more sophisticated with how they deal with their inbox. Our research showed that they look at the from line and the subject line, and they do that very quickly. This is not sort of a long ponderous analysis, this is a split second analysis, and if there's any indication of spamminess, it just gets deleted.

So, I think a big part of the management of this problem, the attitude that Susannah found in her survey, is that consumers have better skills within themselves to cope with the problem, and their service providers and senders are doing better things to help them manage the problem.

MR. STILES: Keep in mind that the metrics around this problem haven't existed for very long.

MAAWG's metric report has been around now for a year and a half, and up until that time, there wasn't such a report that was that extensive that looked across the entire industry at everybody' mailboxes, currently representing 510 million mailboxes on this report.

So, we're just now really starting to put our hands around this problem and understand what the scope is. I think that's difficult for us to look back four years and put numbers and quantify it to four years ago.

MR. GRASSO: One of the changes from a law enforcement perspective, something that I am keyed into that I have noticed over the last year or so and I would be interested to hear any of the people that are involved in messaging to comment on this, but I'm seeing less spam that is actually spammertizing something, and more spam that is either phishing or some type of other malicious attack, malicious software, trying to drive somebody to a malicious website that's going to install a virus or a Trojan on their computer.

I'm starting to see more of that, and I would be interested over the next two days to hear from different people in the messaging community, your thoughts on that. That's just something I'm biased to, because we're concerned about that stuff and that's stuff that's actually happening right now.

MR. HUSEMAN: So, turning to the nature of spam, Tom, as you mentioned, Susannah, what did your study indicate about the types of spam that consumers are receiving now as opposed to four years ago?

MS. FOX: Well, I'm also going to be really interested to hear the data from the industry, because what we do is talk to people about their perceptions. So, when they're talking to us on the phone, it's what they remember about their experience, and so what they remember is that for them, phishing has been pretty much at the same level since 2005, but porn spam, the language really changes when you ask people to talk about the spamvertising versus the porn spam, the language gets much stronger and people say things like, it's hideous, women especially really don't like it.

Luckily that has gone down. The levels of adult content spam has gone down. Really, most people are seeing it blocked, and what I should have also mentioned is that only about less than half of email users actually check their filters to see if there's any false positives.

MR. HUSEMAN: Scott, from the marketing perspective, what do you see now about the nature of spam?

MR. RICHTER: We've definitely seen more of a

shift in messages as more Fortune 1,000 and larger retailer companies realize that online marketing is a big presence and a big part of their future. We've definitely seen that. As her results show, the marketing messages that are being sent are more consumer oriented, consumer friendly, to the users that the people do have an interest in. It's not just all herbal pills and adult content.

MR. HUSEMAN: Charles, what about from your group's perspective, about the types of email, the types of spam that consumers are receiving? How has that changed?

MR. STILES: I think that we see that it has become more criminal, but at the same time, our groups have started to realize that you've got to be careful in the aggression that you use in stopping spam, and in fact, the number of tagged or blocked connections per mailbox has dropped over the past few quarters across our metrics report, showing that we're actually looking at the types of messages that our consumers are receiving, and ensuring that the legitimate messages are coming through, because that's just as important, if not more important, than stopping some of the spam.

MR. HUSEMAN: Trevor, do you have anything to add?

MR. HUGHES: Well, I'm struck by what Charles said, because that is such a change from four years ago. Four years ago, we were rallying arms to fight spam and fight spam only. I think it is an indication that an organization that represents the receivers of the world, MAAWG, and our organization, the ESPC, do work collaboratively now. We recognize that we are joined in this fight, and that the delivery of legitimate mail is as important as the fight against spam, because if we don't protect the good stuff, we are not protecting the very thing that we're fighting for.

So, I'm encouraged by the nature of the debate and the discussion there.

MR. HUSEMAN: Susannah, did your group or did any of the panelists have information about consumers not receiving messages they want to receive because of aggressive filtering or blocking?

MS. FOX: We just had the question about whether you check your spam filter, and it was interesting to see that about more than half of people said no, I rarely check that filter.

MR. HUSEMAN: Something that's definitely changed in the past four years is the enforcement focus, the CAN-SPAM Act obviously passed, at the end of 2003, effective the beginning of 2004, and we've also seen our

first criminal prosecutions against spammers.

Tom, would you talk generally about how law enforcement strategies have developed over the past few years?

MR. GRASSO: Sure. So, when we first started looking at the spam problem back in 2003, it was pre-CAN-SPAM, so we didn't have a law on the books that was going to specifically make sending spam illegal, if you were. So, we were looking at it from a different angle. We were trying to look at, well, is there a botnet involved, are there computer intrusions involved, things like that.

CAN-SPAM came around, and I have to say, from the criminal side, people weren't really ready to rush into CAN-SPAM, as using it as a tool to prosecute. I think that is not because it's a bad law or anything like that, I think it's because when you have a new law come on the books, prosecutors are reluctant to use it as opposed to something else that they know is tried and true. Okay?

I think that's been that way for a long time, it's just common sense. But what we're starting to see now are more CAN-SPAM prosecutions, every day. I'm starting to get more reports from our field offices that they're charging people with title 18-1037, which is the

CAN-SPAM Act, so I think it's starting to snowball now, where we're starting to see people get charged with this, we're starting to see successful cases based on title 18-1037, and more and more prosecutors are willing to employ that and use that as a tool.

Another thing that I will say is that going back three or four years, we started off with looking at these, the people that we thought were the worst out there, and it took a while to build these cases, and we didn't have some successes right away. We're starting to see those successes now, particularly over the last year or so. We've had a number of arrests, indictments, prosecutions, involving some of the worst spammers. So, I think the law enforcement community and the justice community is starting to accept this, that you can go out and that this is a problem. You can get these people, and you can prosecute them for doing this, and good things will come out of it.

MR. HUSEMAN: Charles?

MR. STILES: Being a mailbox provider, it's also interesting to note that we don't often times know exactly what it is that's needed by prosecutors to get this information, so MAAWG has been working with law enforcement officials around the globe, not just here in the U.S., to determine what it is that's needed to go

after spammers and what information needs to be gathered for what term and how to go about doing that. That's something that continues to go on.

We'll be meeting again in October here in D.C., and look forward to another joint meeting with the law enforcement officials to help other ISPs that are our member companies understand what it is that they need to gather.

MR. HUSEMAN: Charles, you mentioned collaboration between partners. What more can we do, what has changed in the past four years and what should we be doing going forward as far as collaborating domestically and internationally?

MR. STILES: I think that we really look at this as a problem here in the U.S. I think a lot of times we try to blame those internationally for creating the problem, but we now are looking at this as a global problem, and believing that the solution will come globally as well.

We are working with organizations across Europe, and also the Asia Pacific region, to help understand what they're dealing with, share what we've learned, learn what they've solved already, and working with their law enforcement agencies so that we understand how we can cooperate with them in tracking down the

spammers.

MR. HUSEMAN: Tom, what's your insight on our collaboration with international partners or international enforcement efforts?

MR. GRASSO: Well, not everywhere has a CAN-SPAM Act. So, when we're dealing with foreign governments, we'll often times have to take a different angle to it, does it involve a botnet, can you go from the content of the spam, does it involve child pornography or something like that that you can get them interested in.

But, yeah, I would say that our international law enforcement cousins out there are the keys to making this happen. The criminal spam is, as someone said earlier, is moving overseas, is coming from overseas. They're using bot networks that are owned by subjects that are overseas.

So, it's these relationships that we're going to build with the international law enforcement community that I think is going to be key to the continued success of this. We're working on that every day. My group does a lot of international travel, as much as we can, getting to meet the other law enforcement agencies out there across the globe.

There's diplomatic channels that can be gone through, but I think the best thing for us, for me as

law enforcement, anyone else in this room that is involved in enforcement, I would say the best thing you can do is develop a relationship with somebody overseas, a law enforcement officer overseas. You are going to get stuff done a lot faster and it's going to be more reasonable the way you're going to get things done as opposed to if you just rely on international treaties and stuff like that.

So, it's very important to develop these relationships and know the people you can count on overseas.

MR. HUSEMAN: Trevor, we've had two and a half years under CAN-SPAM, what is your view as to whether any additional remedies are needed?

MR. HUGHES: Well, gosh, we would like to see regs, that's for sure, the final regs. We're waiting for those on tenterhooks. We certainly have worked very hard on all of the components that have emerged so far.

In terms of additional legal remedies, I'm not sure if applying additional legal standards on the legitimate use of commercial email in the marketplace is where the problem is today. It seems to me that the types of problems that we're facing, the crooks, the fraudsters, phishing, we've got lots of law to cover those things. Whether it's FTC Act, whether it's

criminal, whether it's at a state or federal level, there is lots of laws to cover that stuff, because it's theft, it's ID theft, it's all sorts of things, it's fraud.

So, I'm not sure if additional laws or standards changing or adding to CAN-SPAM is the right way, and in fact I would say that would distract us, perhaps, from some of the more important work. I would much prefer to see more energy, more resources, going into enforcement, so that we can get that deterrent effect. The 6:00 news visual of a phisher with a raincoat over his head coming out of a federal court is a very powerful image.

MR. HUSEMAN: Scott, from your perspective, how has the new CAN-SPAM statute affected the marketplace?

MR. RICHTER: I think overall, it's definitely helped the marketplace, because it's given us a set of guidelines to follow that we know if we follow we're not breaking the laws. The biggest challenge, like I said, that's been growing, and from our standpoint, since we operate a marketing program on the Internet, is that the suppression list issue, as these suppression lists keep growing, I think it was a great idea at the time, but there needs to be some kind of time limit put on suppressions lists, or a better system figured out.

In ten, 20 years, some of these suppression

lists will be hundreds of millions of addresses on them that probably 50 percent of them will already be inactive addresses as users change addresses or don't keep the same address for many years or move on from jobs and different stuff. But that's been the biggest challenge with CAN-SPAM that we've seen.

MR. HUSEMAN: So, I'll leave time for questions, but let me ask one final topic of the panel. Let's talk about consumer education. Susannah, from your surveys and your statistics, what more should we be doing about consumer education or consumers' awareness. Could you expand on that?

MS. FOX: Well, experience is the best teacher, and what we have noticed in the seven years of polling is that the Internet population has matured. Basically we're at a point now where if you're on, you're on, and if you're off, you're off. There's about 15 percent of American adults who are completely disconnected from the network, but most of the rest of us have been online, have been online for a long time and have been dealing with spam and have been learning about how to deal with spam.

I actually am not sure how to reach consumers. You know, I don't have expertise in that area, except to say that we do notice that as people do gain experience,

they gain a little bit in savvy. What we also worry about and notice is that the spread of broadband, we're now reaching about 50 percent of American households with broadband. With broadband comes overconfidence. Everything moves so quickly with broadband, you think that you're kind of a rock star superhero online, and so you take more chances sometimes. So, that's something to watch.

MR. HUSEMAN: Charles, since the nature of spam has changed over the past few years, have we done a good job as a community of keeping up as far as educating consumers about this change? What's your view on consumer education today?

MR. STILES: Well, as far as keeping up with spam filtering, I would say absolutely, it's constantly changing and evolving, but as far as educating the consumers, I think it's difficult for us to expect the consumers to understand all the aspects of spam in this type of an environment when we in the industry are trying to put our hands around it as well.

MR. HUGHES: I would add to this that I don't think it's necessarily sort of direct education, you don't have to send them a brochure or textbook or make them sit through a panel on spam issues, but I think offering consumers more tools will allow them to engage

in and experience that over time they will develop more sophisticated responses to what's happening in their inbox.

Again, our surveys suggested to us that consumers would love to have more than just a report-a-spam button in their inbox. They would love to have a support a spam, an unsubscribe, that was safe and trusted, and maybe even a feedback mode that once a week is okay for this type of message, but don't send it twice or three times a week.

So, giving consumers those types of tools, I think, leads to that experiential type education that Susannah suggested.

MR. HUSEMAN: So, I would like to open up for questions. We have about ten minutes left, and please wait for the microphone so that way the webcast and the court reporter can make sure to hear you. If you can state your name for us.

MR. LEIBA: Hi, I'm Barry Leiba, and I have two questions. I'll try speaking up. I'm Barry Leiba, I have two questions, one is about surveys and one is about consumer education.

The consumer education one is I find it a little bit odd to consider it a consumer education issue that consumers don't know that they signed up for marketing

mail when they bought a product at your website, and I rather look at it as a marketing issue that maybe it should be clearer to consumers that there's an option to get the marketing material and an option not to. So, I would like a comment on that from Scott.

And for Susannah, how do you deal with surveying people on cell phones, which is an increasing issue of people who no longer have land lines?

MS. FOX: I'll take the survey question quick. It's a big problem for us going forward, but the good news is that we are developing ways to survey people on cell phones. We have done some experimenting with that. It turns out to be very important. In the last election cycle, we did some political polling, the Pew Research Center, with a cell phone only population and actually found that although it skews very young, we are now approaching I think one in four people 18 to 25 who are cell phone only.

We didn't notice a change in terms of political affiliations, so that the Pew Research Center was still able to call correctly the last election with a land line survey. That's very different with health surveys, public health surveys find that people who are cell phone only engage in much riskier practices, which I can email you some papers on it.

So, we are noticing that there's a big shift, of course, toward cell phone only, but there is success in terms of getting people to answer short surveys. We have to limit it to ten minutes, whereas a land line, we can keep the person on the phone for about 20 minutes.

MR. LEIBA: Thanks.

MR. RICHTER: In recognition to your consumer education question, I think what the concern is is that a lot of filtering technology is automatically putting mail that people did sign up for and people are aware of it into the bulk folders, and what my concern is is that a lot of these companies have made it very easy, when you do look at your bulk folder, with where you can check all, if it's 50 or 100 or however it's set up, and you just hit submit spam, and a lot of times people aren't reading those messages.

Then at the ISP level, they're just automatically saying, well, if you just sent a thousand emails to us and five users reported spam on the automated report button, then you just must be spamming. I think a lot of times what's happening is that the filtering technologies don't really -- you know, obviously it's all computerized and there's a lot of times there's not a human in there looking at them, so a lot of times anything with an HTML link in it, has an

image, has a postal address or certain words in the subject line, or the body of the email, are just being put into the spam folder.

The biggest thing is then consumers see, oh, you have 100 messages in your spam folder, just click submit all and with the feedback loops that ISPs are offering now, they're just looking at those metrics and a lot of times their metrics aren't changing at the pace that the complaints come in.

I just think it's the ISPs, some of them have done a much better job than others, but a lot of them don't do a good job of saying to the user, are you sure this is spam, did you look at the email, are you sure you didn't sign up, it's just check all and submit.

MR. LEIBA: Thank you.

MR. HUSEMAN: Well, one thing that has changed in the past three years is that my vision increased for allowing ten minutes for questions. So, we have a lot of times for questions and I will intersperse some as well. So, the next question from the audience? Yes?

MR. SCHWARTZMAN: My name is Neil Schwartzman, I'm the compliance officer for sender score served by at the turnpath. I just want to offer some context about the number of complaints from consumers that do block our mail, anyways, the mail that we certify, is

certainly not on the order of five complaints. We offer, depending on the volume of the sender, anywhere between 0.4 percent and up to 2.9 percent of the overall email stream before somebody gets blocked, or off our white list and consequently possibly blocked at the receiving end.

As you know, our white list is used by places like Hotmail, many other -- Roadrunner, a lot of other large receiving sites, and I've got to say that it mistypifies the reality of the situation by saying five complaints are going to get you banned. It simply is not true.

MR. HUSEMAN: So, one question that I would like to ask is about the technological tools. Specifically about authentication. What steps have been taken since our 2004 summit for email authentication from both the sender's perspective and the ISP's perspective and what else can we do? Trevor?

MR. HUGHES: I think there's very good news on the sender side. We require it of our members, the DMA requires it of their members, and we have processes in place to make sure that people are authenticating before we accept their membership application now.

We have seen, I would say, qualified success on the receiving side of the equation. One of the things

that's been true about the problem that we have here, since the very beginning, is that we have a number of very large ISPs that represent about a half, perhaps even more, of inboxes in the United States, and then beyond that, it is tens of thousands of receiving domains. Think of every company, every university, every small regional ISP.

So, we have this sort of split world, where it's very easy for us to talk to the major ISPs, organizations like Microsoft and AOL and Yahoo and are all very much engaged and very much a part of an ongoing dialogue, and are looking at, if not having already engaged in some form of authentication.

But that second half of the equation, the tens of thousands of sites out there, or tens of thousands of receiving domains, that's a real challenge for authentication. Authentication really is only a functional tool if it's used on both sides of the chain. If the sender is authenticating your messages properly, then the sever is using that authentication for something, they are using it to determine what goes into an inbox or goes into a bulk mailbox, they're throwing it into a formula with a bunch of other things to determine whether something gets delivered or not. They're doing something with it.

And, so, while I think we've seen fairly good traction on the largest ISPs, we're still struggling with a lot of ISPs and we're still struggling with consistency across the ISPs.

MR. HUSEMAN: Charles, what's your response to that issue?

MR. STILES: I think the good news is that email technology has solidified a great deal over the past three or four years and they have become much more static and constant and people understand them much better than they did. They now know that these are not silver bullet solutions to fighting spam but rather they are components to a larger set of tools that will help us to combat spam.

From the ISP's perspective, your biggest win is of course getting the large ISPs to implement authentication technologies. The bad news is that when you deal with the largest mail systems, you're also talking about the most complex implementations. Over the last quarter, you're looking at 510 billion messages that need to be evaluated for this type of authentication. So, that's a lot of work that needs to go into our infrastructure.

Now, the good news from that is that most ISPs are looking at authentication or actively working at

implementing and I suspect you will hear more about different ISPs putting those systems into production.

MR. HUSEMAN: Scott, what's your view on email authentication, and in the marketplace, what is occurring?

MR. RICHTER: We've done tests, most of our mail we do use it on, and some of our mail we don't use it on all the time. You know, one thing we've noticed is that with email authentication sometimes is that if somebody has written rules against it, it obviously blocks all the mail you send immediately, and we believe that sometimes they're not blocking the mail because there's anything wrong with it, maybe a filtering company has wrote a rule against our postal address, wrote a rule against something in the email.

So, I believe that it has some benefits if ISPs are honoring it like they say they want to, I think it's very beneficial. If ISPs are just using it to pinpoint certain organizations not to accept their mail faster, then it's a negative impact.

MR. HUSEMAN: Tom, can you talk about the interplay between enforcement and technology, what technological developments have occurred that maybe have helped our enforcement strategies or helped our investigations or what more could we do?

MR. GRASSO: Well, I think first and foremost, it is the authentication services that are out there, the people that are filtering the spam, and providing that service to their customers, also have some great data available to us in law enforcement as to the amount of spam and where it's coming from.

So, if we get to the point where we're targeting a specific spammer and we want to know, we need to reach those levels that are defined in CAN-SPAM, it's the different authentication services that can provide us with that data. You know, we can show them a piece of spam and they can say, yeah, this was a thousand copies of this tried to hit our customers' mailboxes over a couple of minutes the other day.

So, that's really valuable information that they can provide to us.

MR. HUSEMAN: An issue that Susannah addressed was about the sexually explicit spam messages. What changes have we seen in the past four years with that, and, Tom, if you can start out with the law enforcement perspective.

MR. GRASSO: So, I can say that there was a recent case out of Phoenix, which I think a lot of people are familiar with, FTC was involved in the case, and resulted in some successful prosecutions of some

individuals that were charged with not only CAN-SPAM violations, but also charged with obscenity violations, just because of the nature of their spam was clearly obscene and bestiality, things like that, it wasn't your typical type of adult spam.

So, yeah, it's still a problem, it's out there. I think from the government's side, we're willing to look at it from whatever angle we can, whether it be a CAN-SPAM violation or an obscenity violation. I think this is the type of spam that bothers consumers the most. You know, especially if it's obscene, if it involves one of your kids is opening it in their inboxes, this is the stuff that really bothers people, and in fact, what is CAN-SPAM? It's controlling the assault of nonsolicited pornography, yeah, so I mean, CAN-SPAM was geared at this problem and I think this is what bothers people the most.

MR. HUSEMAN: Tom, we have a question from the audience for you as well, what is the NCFTA and how do we get involved and are they focused on issues other than spam?

MR. GRASSO: Absolutely. The national cyber forensics and training alliance is a 501(c)(3) nonprofit entity, it's based out of Pittsburgh, and the best way to summarize it is that it's a neutral ground where law

enforcement and industry can come together and work on cybercrime problems. We do not only work on spam.

Spam was the first initiative started at this project when it was brand new back in 2003, but since then, we have got into all sorts of other things, phishing, stock fraud, which ties into spam, of course, as you all know, pharmaceutical, online pharmaceutical fraud, basically anything, any type of cybercrime that is a big problem for the Internet community and for industry, that's what they work on at this facility.

And what's nice about it is that I get to come to work every day and sit down and work side by side with analysts from industry. There is no walls up, no barriers, we work together. We collaborate on these cases together, roll up our sleeves and work on them, and it's extremely refreshing for me, coming from a government background, to be in that type of environment, and it's also extremely beneficial for us to be able to be working with these great people from industry that have all sorts of fantastic data that they want to share with us on the problem.

As far as if you want to become involved in the project, you can talk to me about it, our CEO, Ron Plesko, happens to be here, he was here, is Ron still here? Nope, okay. Our CEO of the NCFTA is here, but we

do have a website, www.ncfta.net, and you can get more information about the project there.

MR. HUSEMAN: So, one of the questions from the audience, go ahead.

MR. ZWILLINGER: Mark Zwillinger, I'm from Sonnenschein, Nath & Rosenthal. Just a quick question, defining the problem area, we know the FTC is very concerned that one of the problems is inadequate supervision of affiliates, and to what extent an advertiser is responsible for the activities of the affiliates who send the emails on their behalf, and so the question I guess is geared to Scott as someone who runs an affiliate network, I'm interested in your position and to what extent an advertiser should control the action of the affiliates and I also wanted to hear from Trevor whether that view is consistent with how the ESPC looks at sort of affiliate control and supervision.

MR. RICHTER: As far as our affiliates go, when they join our program, obviously they agree to the terms and conditions, part of the terms and conditions is that they don't break any laws and that they'll follow CAN-SPAM. Some of our individual advertisers have different rules on top of our terms and conditions.

Obviously they have to follow suppression lists and different programs, stuff like that, but it's

definitely tough. At any given time if an affiliate of any network or for any advertiser does something unauthorized, we usually, we're very good about taking immediate action, and usually what we will do is we will immediately disconnect the links and have the links go to a page saying this affiliate has been terminated, if they've done something wrong, so at least that way nobody is taken advantage of and they know that action has been taken.

MR. HUGHES: I think the affiliate issue is a very big issue, and I think we probably should spend time talking and thinking about it. Former FTC commissioners describe this as the problem of cascading trust, that an advertisers gives a message to an affiliate network, to an agency, to a partner, and then they pass it and then they pass it and then they pass it, and if it's a cost per conversion type campaign, if they're getting paid, if there's a sale, everyone takes a piece of that commission all the way back up.

The problem is as that connection between the advertiser and the delivery of the ad to the consumer becomes more attenuated across that network, that affiliate chain, the ability of the advertiser to know how it's actually being presented and how it's being sent to the consumer is essentially gone. While

contractual provisions are the predominant mechanism for an advertiser to try and gain some control, I don't think we have seen a lot of auditing and accountability from advertisers in terms of really getting out there and managing how their messages are being perceived in affiliate networks.

And I worry, I worry that advertisers not only may be exposing themselves to legal risks because under the CAN-SPAM Act, one of the more inspired policy choices was that the sender of the messages, the advertiser, within the message, not the company that hit send, but the advertiser, within the message, the advertiser can be on the hook for those practices of that terminal end of the affiliate chain actor, and those practices may be pretty nefarious.

So, I think that there certainly is room for us to be looking at those practices. We don't have best practices in that space, but it's certainly something that we talk about quite a bit with our members.

MR. HUSEMAN: Charles, another question about what's on the horizon? We've talked a little bit about what's changed? Now we're hearing about image spam, PDF spam, and technologically, what are we doing to look ahead and prepare for the next evolution?

MR. STILES: Really we've just got to keep our

eyes open, and it's something that evolves and changes, not only a day-by-day, but on an hour-by-hour basis, and as we continue to see these changes come up, we find different ways of combatting them.

What's the future hold? I don't know. I don't think any of us can know for sure. I suspect that botnets are going to continue to be a problem for quite some time, because spammers have moved from the basement into our own living rooms and taken over our own PCs. I think that that's going to pose a problem for us for quite some time.

Now the method they use for delivering their message, whether it's image, whether it's an application, whether it's PDF files, that remains to be seen.

MR. HUSEMAN: Does anyone else have any thoughts on that?

(No response.)

MR. HUSEMAN: Tom, if you can speak specifically, have you contacted, when you've contacted consumers whose computers have been compromised, I mean I assume they're often unaware of that. What's been the reaction?

MR. GRASSO: They're usually unaware. They say, oh, boy, I noticed it's been running slow lately, so

that's the complaint that you get. But they're often unaware of what exactly is going on. The computers that are being co-opped to do this stuff, the malware is really good at hiding itself. Easily from your average user, but even sometimes from people that are computer experts.

So, these people don't know it's on their computer, they just know it seems to be operating slowly, and that's mostly because their Internet connection is the bandwidth has been soaked up with all the spam that it's blasting out.

So, what we try to do is with the help of our industry partners, obtain permission, authorization, from the user to monitor that computer, to get them to run some forensic tool that some of our industry partners have developed that they can easily put on their computer, create a report, give that information back to us to show, yeah, okay, this computer is infected with something, but who is it talking to, where is it getting its commands from. That's what we're interested in.

But to answer your question, yeah, they often don't know until they get a call from us or from the ISP.

MR. HUSEMAN: Do we have some questions from the

audience? Please wait for the microphones.

UNIDENTIFIED SPEAKER: This is a question strictly as a computer user, my computer may be compromised, can I contact you, is that something that I can send to you or something that you send to me to help me know whether I can find out?

MR. GRASSO: Okay. Well, there's a number of websites out there that can help with this, and the first one that comes to mind is a really great industry partner of ours, Lawrence Baldwin, he has a website called myNetWatchman.com, and if you go onto that website, you'll see they have a tool on there called SecCheck, and that's something you can download and run on your PC and it will look for malicious software, for signs of infection on your PC, and then it sends that information back to Lawrence and he keeps all that in a database that he can share with law enforcement if we need it and things like that. That's one thing to do.

Joe, can you think of anything, any other sites that are good at that?

MR. ST. SAUVER: Lawrence's site is certainly one of the best.

MR. HUSEMAN: Can we have the microphone?

MR. GRASSO: This is Joe St. Sauver from university of Oregon.

MR. ST. SAUVER: Lawrence's site is certainly one that I would recommend, but I will say that there are also many other industry partners out there who have good tools, many of the anti-virus companies offer free anti-virus fix that will take care of some of the malware that may be on your computer, and there are increasingly anti-virus tools that are also available. Google has many of those tools and will make them available to you.

MR. GRASSO: Here's the problem, and in fact, that the work that we're doing on law enforcement and we're undercover and we're in these different forums where the virus writers are hanging out, they're writing malicious software and they're marketing it on the fact that it's not detected by any of the virus definitions yet, okay, so they're writing this stuff, and they test it against all the popular AV software, and then they advertise, hey, I just wrote this new virus, it's not detected by anything, who wants to buy it from me, okay?

So, this is part of the problem. So, it's kind of like, I guess to answer your question, it's like a catch-up game. You have to keep checking your machine and if something is on there it's probably going to get detected, maybe not right away, and I think that's probably the best thing that you can do.

MR. HUSEMAN: Some more questions from the audience? Yes?

MR. RAMASUBRAMANIAN: My name is Suresh Ramasubramanian and I manage the spam operations for Outblaze, we are a Internet provider.

MR. HUSEMAN: Can you speak up just a bit, sir, please.

MR. RAMASUBRAMANIAN: My name is Suresh Ramasubramanian and I manage the Antispam Operations for an outfit called Outblaze and I would like to point out one fundamental thing that a lot of the panel has been discussing, but with authentication is pretty good in its own right, but while we are looking for a cure for all spam, or we are recommending that, for example, email marketers use authentication to declare that the mail is coming from a particular IP space, it's usually kind of limited in this area, because while it creates much more standardized way for us to know where a marketer's email is coming from, quite often, if a marketer gets blocked, he's getting blocked because of complaints from his own actions, shall we say, from email that he sends out.

It's not like where it's a bank or a financial institution or something that is getting impersonated by people sending from botnets and, for example, ebay and

PayPal and I'll safely say that we sign all of our email with domain keys, and if you see email that claims to be from us and it's not signed by us, feel free to trash the email.

So, I'm looking at how useful authentication is for a marketer beyond just declaring to an ISP that we are going to be sending from this range? They are normally sending from that range and they are reasonably static sources, it's not like they skip around from China to Brazil or to India to somewhere else and it's just like a botnet. So, how useful is authentication beyond that?

MR. HUGHES: So, I can respond to that. Hi, Suresh. We never saw authentication, the ESPC has never seen authentication as a silver bullet, we have seen it as a dispositive mechanism for deliverability into the inbox, and certainly it has not become that in the marketplace today. But we do see it as one factor that can be used by ISPs in their broader mix of factors to determine what should go to the inbox or the junk box or be blocked outright.

It's one more indicator that the legitimate marketplace is acting competently and consistently, and that is what helps to engender trust. I think over the past four years, we have seen particularly on the issue

of email authentication, that the sending community and the receiving community have found common ground to talk about many of these things and that's led to greater trust and greater discussions on all sorts of stuff.

So, we've never seen it as a silver bullet, your points are very well taken, that for marketers it's not dispositive of inbox delivery and should not be seen that way. I still say, though, and we still require that our members and that any marketer that's trying to do things the right way should be authenticating their messages.

MR. STILES: I think you need to make sure that you look at authentication as a key component to a reputation system. Authentication by itself doesn't mean that you get a pass or a fail, it's really about attributing a reputation and we need to remember that reputation can be both good and bad.

So, the benefit to a marketer is to be able to rely on their good reputation and bring up new IP addresses which he may not have mail for or be mailing under perhaps a different name than what they've mailed from before and benefit from that positive reputation and the good practices that they've upheld to that point.

MR. SPIEZLE: Craig Spiezle from Microsoft. I

want to follow up on that comment, and again, authentication is the first part. It's a driver's license, and reputation, as Charles mentioned, is very important, and that's the driving record. Sorry, I'll speak a little louder.

So, but specific to the point there, so what we're finding today, with marketers who authenticate and have good reputation, actually their false positives have decreased 85 percent, and the reason is, it gets into the mix that Trevor mentions, is we're able to take the result of a good reputation and apply that to the mix, and so an example of a bank or a financial institution, their mail may get junked because the content with the financial data, their positive reputation could override that and make sure it's delivered. But we have a key success there.

The other part I think I want to challenge is that while it's great that marketers are doing this, we need to go a step further and get the brand owners and the domain at the higher level. It's not just about the email marketing domains, it's about authentication and reputation, it's protection from the deceptive and the forged mail which is coming from other sources.

MR. HUSEMAN: I have a question from the audience. Botnets are recognized as a tremendous

problem, are ISPs quantifying the number of botnets on their network or the percentage of users, and are they taking steps to remedy the problem?

MR. STILES: Just speaking on behalf of MAAWG, we do recognize it as a problem, we do have a botnet subcommittee that's evaluating the situation. We have not released any metrics on botnets specifically, and the extent to which we resolve a botnet problem really varies from ISP to ISP, because there are a significant number of resources that are required for resolving that. Everything from walled gardens, actually making consumer calls out to the customer, even home visits, and it really varies from ISP to ISP.

But yes, it's recognized, it is being dealt with, and is being evaluated even further to see how we can combat it more effectively.

MR. HUSEMAN: Tom, in the law enforcement experience generally, what has been the prevalence of botnets in your investigations?

MR. GRASSO: They play into just about all of our cybercrime investigations in one way or the other. I mean, this is what the criminal spammers are using to send their spam out, they're not sending it from some mail server that they own somewhere, they're sending it through a botnet to hide where they're coming from. The

prevalence of botnets is increasing, their sophistication is increasing and the size of them is also increasing.

Microsoft has a project that they call the Botnet Task Force, which I know all the Microsoft folks here are familiar with, which they've put together that's enabled us in law enforcement to team up with the different industry folks and attack this problem. Now, I think the official Botnet Task Force meeting is going on right now down in Australia, so I don't think there's anyone here from the Botnet Task Force, but does anyone from Microsoft want to comment on that, what you have seen through that initiative? Or I have the wrong people here, okay, I'm sorry.

No, it's on the rise. But we're getting better at identifying these and detecting these and sharing the information as to where they are and some of the ISPs are really good at getting them shut down, too, when a command and control mechanism is identified, they are getting really good at pulling the plug on that and getting it shut down.

But there's guys out there, and just so you know, these botnets are not deployed by the spammers themselves, there's guys out there that this is what they do for a living is they build these botnets and

they build them by sending you an email message that's got a link to a malicious site, you go there and your computer gets infected and now you're a bot, okay, and you're reporting back to this guy's command and control server.

Now, what he does then is he sells time on that bot, okay, kind of like how in the old days you had to pay for time to use the computers and stuff like that. Okay, he will sell you like a week on his botnet, he will sell you two weeks, whatever you want to use and you've got his botnet to send out whatever you want. You can spend out spam with it, you can D-DOS someone with it, whatever you want to use it for, it's there for you to use. But these guys build these and then they sell time on them. It's a business for them.

MR. HUSEMAN: Other questions from the audience? Yes?

MR. FENTON: Hi, I'm Jim Fenton. Scott Richter mentioned in his remarks that one of the issues that he's seeing in terms of deliverability is consumers who have, in fact, opted into receive some messages, having forgotten about that and hitting the spam button when they receive these messages. Do you see a need to increase the stringency of opt in, perhaps to double opt in or something like that, either as a best practice or

as a requirement in order to avoid that problem?

MR. HUGHES: I'm happy to answer that based on some research that we did earlier this year and I actually want to mention a tool that Microsoft has created as well. What our survey found earlier this year was that consumers use the report-a-spam or complaint button as a single button, as the only tool available to them to respond to something that maybe they asked before, but they don't want anymore, and they're not as frequently using the unsubscribe function found in the email itself. In fact, we may have created that reality, because for many years, the marketplace was telling consumers, don't unsubscribe from emails, you're just verifying your email address for the spammers so you will get more.

So, consumers at least have that legacy of knowledge that okay, I'm not supposed to unsubscribe from the email itself, but my provider, my email client has given me a button here that says report a spam and I'm smart enough, knowing my email client, that when I hit that button, I know that that means that I don't get stuff from that sender anymore. I don't know if that's blocked, I don't know if people go out and arrest that person, but I know it doesn't get into my inbox anymore and that's okay.

So, frequently they're not reporting it as spam, they're just using it for the de facto result of what happens when they hit that button. We think that consumers need more tools.

So, I wouldn't put the solution on the consent part of the process, because the consent process seems to be working well. The consumer knows that they asked for it, they just need a better way to say they don't want it anymore. So, we applaud Microsoft as being one of the few ISPs that's actually implemented an unsubscribe button.

So, it is helpful for consumers to be able to distinguish between reporting something as spam and just saying I don't want this stuff that I asked for before, I just don't want it anymore.

So, I would encourage more ISPs to move in that direction as opposed to us looking at the consent side of the equation.

MR. HUSEMAN: So, I would like to go down the list of panelists and ask you all the same question. If you could briefly define, summarize, what is the problem today, and how has it changed in the past four years?

MS. FOX: I would say the problem is the loss of trust in email that we consistently find that people say that spam is making them trust email less, and so I

would say that's the major problem from our perspective.

MR. GRASSO: What Susan said, yes. No, absolutely. I think it's diminishing the trust of email, its usefulness as a business tool, these are all being affected by the spam problem. How it's changed over the four years just to reiterate some of the stuff I said earlier, at least from what I can tell, it seems to be more about malicious software, phishing scams, other types of things other than just, oh, hey, we've got a product that we want to sell you. There's like a lot of other stuff going on behind it, manipulating the stock market, things like that.

So, we've got a whole host of other bad things that spam is being used for where I think at one time it was just about marketing stuff and I don't think that's the way it is anymore.

MR. HUGHES: So, I am going to agree with Susannah and Tom. I think four years ago we had this big, ugly bucket of all sorts of things that were going on, malicious activity, things that were sort of early forms of phishing, but also the mainstream marketplace didn't have standards, didn't have a lot to look to really, we had all sorts of state things that were being applied to us.

What I think we have changed in the past four

years is the legitimate email community has recognized the need for it to protect email as a whole, and the use of legitimate email as a subset of that whole, and they have pulled themselves out of that ugly bucket of mess and have developed standards, the best practices that we have, we've developed technological tools, like authentication and replication systems and there is broad compliance with the CAN-SPAM Act.

That leaves, I think those things that Tom has described, the more malicious, fraudulent criminal activity as being major problems for us. That's not to say that there's still not work to be done, and in fact, I think one of the interesting things that's changed over the past four years is that as we have brought sort of mainstream email into the bright light of day and given them standards and they are adhering to those standards, we found that, and there's probably 20 or 30 of them in this room, that we need deliverability experts to actually manage email for big companies now, and many of our members provide those services to their companies, the folks who participate on our calls are the VPs of deliverability, directors of deliverability, who have within their realm of responsibility compliance with the law, technological updating and compliance with technological standards, and actual relationships with

some of the bigger ISPs, talking to people like Charles on a regular basis.

So, it is a much more professional, much more sophisticated business environment today with still some of these criminal and malicious threats on the fringes that cause us all great concern.

MR. HUSEMAN: We just have a couple of minutes, so Scott just briefly.

MR. RICHTER: I agree with what Trevor said, and as the landscape changes more and more and what's happened over the last couple of years going forward, it definitely makes it much easier having guidelines and rules to follow, the only downfall is that legitimate email marketers still do get mixed up with people who do phishing or malicious stuff, and until a lot of filtering companies can understand the difference, it's quite challenging because unfortunately, legit marketers pay the price for it because it's easy to identify now that it is identifiable, versus mail that does come off of the bot networks.

MR. STILES: Bulk is still a four-letter word, but it's not a bad word, so that's probably the biggest change that's happened over the last couple of years. Legitimate marketers don't have to be skeptical about disclosing lender mail and what they're mailing and

there's a collaborative effort between them, and the spamming activity has moved literally from teenagers trying to make a quick buck in the basement to actual criminals who have lots of resources globally and will stop at nothing to deliver their messages.

MR. HUSEMAN: I would like to thank all of the panelists and we will reconvene again at 11:00 a.m.

(Applause.)

(Whereupon, there was a recess in the proceedings.)

EVOLVING METHODS FOR SENDING SPAM AND MALWARE

MR. HODAPP: If everyone would take their seats, we would like to get started. If people could please take their seats so we could begin with the panel. The longer this takes, the later lunch will be. Or maybe no lunch.

Okay, just less than a minute.

Okay, I would like those of you who perhaps have unmuted your cell phones or wireless devices to mute them again, please. This is the second panel of the morning on the evolving methods for sending spam and malware. My name is Lawrence Hodapp, I'm an attorney at the Federal Trade Commission. The case I've done that's the most pertinent here is the case against William Dugger who the chairman mentioned in her remarks. Dugger was using a botnet to send sexually explicit spam.

The goal of this panel on evolving methods for sending spam and malware is to highlight this interrelationship between malware and spam. So, we'll be talking about the more criminal variety of spam that was discussed in the first panel. Not only do we want to try to discuss the status of the methods being used today, we also want to try to give you some of the factors that we think may govern the evolution that's

occurring. What are the pressures?

We have an extremely well qualified panel to discuss these issues. I will mention some of their affiliations, but you understand that the views expressed are their own and not necessarily those of their organizations.

First here is Patrick Peterson, Patrick is a vice president for technology, IronPort Systems of San Bruno, California. IronPort provides security products and services for web and email. Patrick works in the development of these solutions and is a frequent speaker at industry events and a writer on security issues.

Next to him is Joe St. Sauver, Joe is the manager of security programs at Internet2 on contract from the university of Oregon. He is also a senior technical advisor to the Messaging Anti-Abuse Working Group.

Next to him is Jon Praed. John Praed is an attorney and a founding partner of the Internet Law Group of Arlington, Virginia. Jon has represented AOL and Verizon in some precedent-setting litigation that has held both spammers and the websites that employ them liable, including monetary liability, which is of course the best way to make them aware of the need to comply with the law.

Next to Jon is Ben Butler. Ben is the director of network abuse for GoDaddy.com of Scottsdale, Arizona. GoDaddy is the world's largest domain name registrar and also a major provider of web hosting. Ben has a background in network and email administration and he directs GoDaddy's zero spam policy.

Next to Ben is Suresh Ramasubramanian. Suresh is the manager of anti-spam solutions for Outblaze Limited in India.

MR. RAMASUBRAMANIAN: Hong Kong.

MR. HODAPP: I'm sorry, Outblaze is based out of Hong Kong?

MR. RAMASUBRAMANIAN: For now, I am working at home, I have a small kid to take care of.

MR. HODAPP: You don't have to work where the company is these days. Outblaze is the largest provider of email in the world. Suresh is responsible for the spam filtering and blocking decisions that affect their 40 million email accounts. He was highlighted in Business Week in 2002 as one of the 25 top e-business professionals where they dubbed him the chief junkmail zapper.

The panel has decided to proceed with three presentations, after which we will have a substantial amount of time to discuss the topics raised in those

presentations. Starting with Patrick Peterson, then Joe St. Sauver and then Jon Praed. There's cards in your packet that you can fill out and will be sent forward, in addition to having questions and answers from the floor at the end of the presentations. Likewise, people on the webcast can submit their questions as described earlier.

Now, Patrick, if you want to go ahead, we'll proceed.

MR. PETERSON: Thank you, Lawrence. I'm very excited to be here with what is certainly going to be the best panel of the FTC Spam Summit, I'll just lay it down right now. I should also make one other mention, my owners are here, that is to say Cisco Systems, and the transaction to acquire IronPort closed between when I was invited and now, so I want to make sure that my new owners get the credit for now owning IronPort Systems, but as Lawrence mentioned, we had a bit of a struggle with this panel. He got together with us, he explained what he was looking for and he explained very much that he wanted people who didn't have Ph.D.s in spam to get a lot out of it, but he didn't want the people with Ph.D.s in spam to be bored.

And so we went off, talked about a lot of things and came up with a lot of great ideas and came up with a

really good solution for him. We said, our panel right now is at one and a half hours, if we could have one and a half days, we could really do justice to these topics. So we came up with a compromise, I think he cut out like 30 seconds of his intro and we came up with this alternative method. What the alternative method is is that I am going to spend about 12 minutes and I am going to do the training wheels version.

This is going to be the framework for understanding maybe not simple but more basic things, and the idea is that that will become the framework on which a lot of the panelists will rift and go into a lot of the more complicated, interesting things.

So, let me begin with this slide. I believe that if we look at all of these complicated issues to the right lens, it gives us a tremendous advantage in really understanding the issues. This is the lens that I use.

First of all, capitalism. Spammers today are capitalists and they are very talented and genius, they may be evil criminal, but they are talented and genius capitalists, and what they are doing is designed to maximize their profits. In particular, we are going to use some examples throughout my training wheels presentation from a group that I call My Canadian

Pharmacy, also known as the Yambo gang.

We estimate that they are doing over $100 million in profit today from illegal pharmaceutical products. Clearly you don't get to that scale of business and stay out of the arms of law enforcement unless you're pretty darn good at knowing how to make money.

The second thing, of course, then, is if you want to make money in spam, you've got to get it in the inbox. The third thing is that once I, if a were spammer, get it to the inbox, the next thing I have to do is to actually have you take action, to get your money, to infect your PC, what have you.

Again, so far, so good, it sounds simple. The problem is, it gets very complicated, for the reason listed on the slide. Spammers are actually operating in an incredibly hostile environment. We're trying to block their mail, we're trying to shut down their servers, we're taking down their websites, trying to put the handcuffs on them, trying to shut down their affiliates.

And unfortunately, they haven't said, boy, this is a pretty tough gig, we're going to give up and go get a day job at Starbuck's or McDonald's or wherever it may be, they have responded by adapting, and they have

adapted incredibly richly and quickly, which means that a lot of these things which look straightforward can be very complicated because of the way that they are innovating.

So, this is our training wheels version of the framework for understanding the spammers on which we will kind of base the more advanced conversations. The first three items are how they deliver the mail. They need your email address, if they want to get it in your inbox, they need the content and they need some way of firing lots and lots and lots of these messages out, and of course today they're using bots.

Items four through six are the actual action. They need you to respond to that spam, it may be to buy a stock, it may be to go to a website, it may be to call a phone number for a diploma, but they need you to take action. So, they need some kind of infrastructure for that, and in some cases spam actually has a payment directly to the spammer or the affiliate, and in other cases they actually deliver product, and so in some cases they need those as well.

Now, again, I'm going to try to keep it very simple and basic. I know a lot of the people with Ph.D.s are going to be raising their hands and saying that's oversimplifyied, but I think Joe is going to have

a pretty amazing presentation where he is going to put together the way the eco system really works that they have adapted to add a lot more color to this.

So, start with the top three methods of which I have listed four here, for those of you who are proofreaders in the audience. The first thing you can do is you can go online and you can Google or Yahoo or Microsoft search for email addresses and you can find people will sell 40 million email addresses for $40.

The second thing you can do is if you're a bad guy and you've compromised someone's PC and are running software, you can just grab the address book of all the people that they email to and that's a nice list of email addresses that allows you then to send email and make sure it gets put in someone's address box.

Directory harvest attack is another technique and I am going to talk about that in more detail, and last but not least, you can go to a website and if someone has an email address on that website, you can actually purchase a tool, again online, very easy to find, through search. A tool that will go out, spider the web and come back with all of the email addresses on the Internet or perhaps just targeted ones for the people who are most likely to buy your product.

Since often times I think the directory harvest

is discussed and then maybe not well understood, I would simply give a very simple example of how the directory harvest works. The way I thought would be best to explain it was actually to give a postal mail example of how this would work if spammers wanted to get postal mail addresses.

So, in this case I have hypothesized that a spammer really wants to know who is actually working at the Federal Trade Commission, so that they can send them lots of bulk postal email. So, in this case, they may put together a bunch of names and addresses like these, pop them in the mailbox and go on vacation for a week.

When they come back, they may find that their mailbox at P.O. Box 666123 Spammer Court in the Ukraine has a bunch of mail that was sent back to them because it was undeliverable. It turns out there's no Deborah Jones, Jim Smith, James Jones or Lawrence Smith, hypothetically speaking, working at the FTC, so the FTC sent those letters back to the spammer.

What the spammer then does is he puts the two together, knows what he sent, knows what came back, and the difference is real people who work at the Federal Trade Commission and the next time you mail to those six people, you know that it's going to be delivered.

This is exactly the same thing that they do in

the email world. They actually have a server, it's a bot, and it may be my uncle or aunt if they're not careful with what they do with their email on a new PC, and they program these things without my uncle or aunt's knowledge to go and connect to the Federal Trade Commission or Cisco or Comcast or wherever it may be and say, jsmith@comcast, jsmith@cisco, j.smith, d.majoras, Deborah Majoras, Deborah_Majoras, whatever it is, and they'll basically go through the alphabet, they will go through first name, last name, and they will figure out, based on the response, yes, send me the email, no, this person doesn't work here, what the actual addresses are.

Now, of course, in this online version, though, they have some advantages, they don't have to wait a week, it's realtime, they don't have to spend $3.69 on stamps for every nine ones they want to check, and of course it's all done without them needing to control the server which is doing it.

So, that's again our very quick overview on how these email addresses are obtained, and I'm sure the panel will have a lot more color on that.

They've got the email addresses, now they have to get the content in the inbox, they have to get it past the spam filters and they've got to get you to take action. Today, as Special Agent Grasso mentioned,

they're trying to sell and get you to do lots of different things. In the case of 419, it's the niece of the former emperor of Nigeria who has $30 million in a bank account and just needs your help, perhaps someone over in Italy has won the lottery and needs your help, and there's lots of other kinds, selling you pills, selling you diplomas, what have you.

In addition to the types of spam, there's different techniques that they use to ask you to take action. The reason that we emphasize these is the technique they use to ask you to take action is often the one which we on the security side use to identify the fact that it's spam. Those are examples like a URL spam where you click on the link to a website, an image which doesn't actually have any textural links, or maybe it's just text.

So, what I was going to do now is give quick examples of pharmaceutical spam and stock market spam and some of the ways that they commonly use these techniques to be successful in that business.

So, I mentioned earlier, My Canadian Pharmacy, very large, successful, $100 million, $150 million business a year, this is an example of one of their spams. It tells you the products that they are advertising, it asks you to take action by clicking on

the link and it throws in some excerpts from The Hobbit. They've got the software that they use to send this program to take different pieces out of the text of The Hobbit so that spam filters may be confused by this legitimate-looking text in the message.

Again, the idea behind this is if you click on the link, you go to the website. This is the content that they are trying to get you to take action to visit the site. Since we're doing the training wheels, I won't dwell on the sophistication, but we've seen tremendous innovation from this organization in getting their spam delivered. We've seen them changing the domains that they use in spam every 15 minutes. We've seen them changing the content in the spam every 12 minutes, phenomenal innovation in the spam content in order to get it delivered, because if it's not delivered, they're not going to make any money.

There's a second technique as well which they commonly use. Now, this is still asking you to go visit a URL, but a lot of really smart people on the anti-spam community have figured out how to look at an email message and say, this is asking someone to visit a URL, let's take a look at that domain and let's figure out is it good or bad, was it registered recently, is it safe or not.

And so what they have said is, well, we're going to get rid of the text version of that domain in the email. So this is an example of a spam which is an image, it's a gift with no text whatsoever that can be read by a machine, short of the rather complicated and problematic optimal character recognition technique where you actually render the image and try to interpret it.

In this case, they're actually giving the end users explicit instructions. You can't click on this link, you can't copy and paste the link, you have to actually read it here, open your browser and type it in to visit it.

Again, the action that they want you to take is the same, go visit this website, we've got a great deal on herbal Viagra, or some other kind of Viagra, but they've eliminated the presence of the link in the email, by putting it inside an image, to try to increase their deliverability and get past the spam filters.

Now, I'm going to talk briefly about another kind of spam which we've seen a lot of and that is the stock market spam. In this case, they're running the pump and dump spam, they've acquired some shares at a low price, they figure if they send out enough of these messages, there's a sucker born every minute and someone

is going to decide to put their retirement savings into one of these stocks, the more people who buy, the more the price goes up, and they sell it at a profit. Old technique, it's been around for a long time.

This was an epidemic in 2006 and I will give some stats in a minute. The reason that it was an epidemic is they found methods to use images to increase their deliverability to very high rates. I also think that they found perhaps some weaknesses in the way that our brokerage systems and whatnot are used.

Now, three or four years ago, if I had been here giving this presentation, again, lots of hands would have shot up and said, we know how to stop images, we use the concept of fingerprints. Right now if you enter a secure building, you put your fingerprint on there and they compare your fingerprint with a database of good and bad ones and figure out whether to let you in or bring up the gates and call security.

We used to do the same thing with images. You take this image, it's a bunch of zeros and ones that's encoded as a gift and you basically do a fingerprint of it, also known as a check some or hatch. You then say, this is a spam, I've got its fingerprint, I am going to look at all the messages that come in with information and I am going to look at fingerprints and if it's the

same fingerprint as a bad image, I know it's a spam and I throw it away. So, again, unfortunately the spammers didn't take our security response and give up, they came up with something different.

This is an example of the very same image we looked at, which was trying to get people to buy Goldmark Industries, highlighting some of the features that were not very visible to the human eye, namely these small dots inside the image. They take an image, which tells people to buy Goldmark Industries, and they create many, many, many copies of the image, they all look the same to your eye, but they all have dots in different places. The human eye sees it as the same, however a computer, when it interprets it, the actual encoding of the image is very, very different, even though there's only a few dots.

Many, many other techniques that they use so that they basically get the same message out to lots of consumers but they do it in a way that the fingerprinting technique we used to use for images is no longer useful. So a lot of people had to go back and develop new techniques in 2006, and while different companies were doing that to protect consumers, they were getting a lot of these delivered and they were making a lot of money.

Again, talking about spam types, on the left, we have a text spam, which is telling people to buy Goldmark Industries, on the right, we have an image spam, in the middle of that is actually an image, and if you look closely you can see the little dots and lines that they use to make the image different inside the gift and coding, but in addition, they've got text above and below the image which was randomized to try to confuse spam filters, and then down at the lower left we have a text spam touting Goldmark Industries, but it actually includes a legitimate press release. If you go look up that press release at the bottom, it's actually a true statement, it's on their website, they did procure distribution rights for the film in question, so now there may be legitimate copies of this press release going out and they've attached those to their spam, which is touting the stock and the likelihood that it confuses spam filters to get it delivered. A few examples of what they're doing today with the content of their message.

Now, Joe later on is going to tell you why it's not nearly as simple as I present here, but again, I'm going to keep the training wheels on and say, here's what happened. At the lower part of the screen, I have an excerpt of the spam, which you saw a minute ago, most

of the time spam lies, in this case it tells the truth. It's saying, there is going to be a big advertising campaign in early July around Goldmark Industries and the price is going to go up.

Sure enough, in early July, there was a big advertising campaign, they dumped hundreds of millions of spam touting their stock into people's inboxes. The result is shown here on this graph that I got from Yahoo Finance. It shows that a price of $4.75 was the price for Goldmark Industries until July 3rd, when the spam started touting the stock the price went up to $8.50.

This is an example of the success that people have had in using spam, particularly the image spam technique, to tout a stock, to have people purchase it, to artificially inflate the share price, and then to sell it at a significant profit.

Now, I have to say, many times I am somewhat pessimistic and somewhat frustrated by our inability to put a lot of these people in jail, but just yesterday, I think there was some wonderful, wonderful news, and that was that the SEC indicted two people, that are the Usalatins [ph], in Texas, for this type of fraud. They had actually made, these two gentlemen in Texas, they were recidivists, they had been prosecuted for this type of thing before, $4.6 million in seven months and it

looks like the SEC has a very good case against them.

(Applause.)

MR. PETERSON: Yeah, are there people from the SEC here today? Anybody from the SEC who can identify themselves? Drinks on us for all the SEC people who did a great job there. One really nice success story.

And the last thing I want to comment on here is some statistics around the content in spam, the one thing I'll emphasize is the growth of image spam in 2006, and the other thing I'll emphasize is I don't think these statistics really matter. I've got some statistics from IronPort, I've got some statistics from MAAWG, the group which Charles Stiles chairs. You can go get lots of statistics from Symantec, from McAfee, from Trend, from a dozen other vendors. They're great reading, they are very interesting, but fundamentally, I think we can all agree, any set of those statistics show that the problem is large enough that action is needed.

So, that's the one thing I'll emphasize and the other thing I'll emphasize is whatever the technique is today, the technique du jour, we'll respond to that, they'll come up with a new one. We have to think about it that way, and not think about it as image spam is a tough problem, let's stop that and we'll all be happy.

So, next, we'll get to the last kind of meaty

subject, and that's the bots. The first thing is how the criminals have evolved. So, I will get, and I haven't actually done this, but if I was working for the Drug Enforcement Agency down at the Mexican/U.S. border, from time to time there would be people driving drugs in across the border to try to get them in the U.S. If those people were arrested, they would find that those people were not the kingpins, those were not the ones actually making most of the profits through these illegal activities.

If you're a criminal, that's a wise move. Let's have someone else take the rap, someone disassociated from me so I can reap the benefits without the risk. That's the exact same thing criminals have done as they've moved from their infrastructure, their servers, which they used to pay good money for, to run and send spam in 2000 and 2001, to instead using consumers' PCs for that purpose.

So when Special Agent Grasso kicks down the door and goes in there to arrest the owner of the bot, he finds my aunt, who double clicked on an attachment and is in no way a party to the crime, but now he has to go beyond the computer sending the spam, behind the bot to actually get to someone.

So, it's really, again, a clever technique,

which has been very successful for them.

What is a bot? A bot is simply a computer, which is running some application software to send spam, without the owner's knowledge. I could have this PC host a website, I could have it control a machine tool, I could have it play an audio visual file, I could have it send spam by installing that software.

And again, I've got some Hughes statistics, and later on the panel is going to talk about the more complex things which bots do. But let's just answer the question at a very high level quickly, who in the world would go install this spam sending software on their PC? The answer unfortunately is a lot of people. Why are they doing it?

So, on the right, I've got the picture of the Trojan horse, this is how the Greeks finally besieged Troy, after ten years of Odissius and others pounding at the gates, they simply left behind this gift and sailed away. Inside this gift, of course, were the Greek warriors, and once they were led in through the subterfuge, they then took down the city.

On the left, I have the modern day Trojan horse, actually this is two years old, which is ancient in modern online crime, this is an email that purports to be from the FBI, to try to get people to do what the

Trojans did, thousands of years ago, double click on this complaint from the FBI, which then infects the computer, and then they've actually installed this spam-sending bot software and maybe ten or 12 other nefarious things and now their computer is owned by the bad guys.

That's what's happening today, generating all these bots on the Internet. One other thing that I want to comment on, very quickly, botnets is simply a network of these bot computers, which are controlled by the criminal, for all sorts of things. The panel later on is going to talk about bot university, which is more and more sophisticated things bots are doing to communicate without us being able to check them and to be able to send spam effectively for longer periods of time.

Then in particular I am excited about Ben, because I focused on bots to send spam. They're starting to use web servers and web forums to send more and more spam and I think he's got some real expertise there on kind of a cutting edge area to show.

Last comment is I want to give two quick examples of what bots mean to us. The first one is holding up a mirror to the bot computers on the Internet, and in particular, the large service providers. Now, I don't mean to pick on any of our

large service providers, they're all working very hard, but the problem is they have the most consumers with the least knowledge, they do not have a professional IT staff to come by every day and take a look at their desktop and their firewall, and so they are the ones that are getting infected, and when they do, there's no one there to help clean them up, unless perhaps they have a young relative who works in high tech. Other than that, they've been on their own.

So, what we have done is we have actually held up a mirror to the Internet and said how infected is the Internet? Now, this slide is a little complicated, but the simple way to understand it is this is what a large enterprise sees coming to them from the Internet. So, this is a screenshot from an appliance, which is receiving Internet email, at an enterprise, and it's basically saying, in the last 24 hours, they tried to send, the Internet, eight and a half million messages.

Now, which were the networks, which were the collection of PCs which sent the most? Well, number one there is Polish Telecom, it tried to send this enterprise 401,000 messages, of which seven were legitimate. You can go down the list for yourself, the point is, if you look at the mail coming out of the large broadband consumer networks, it shows you the

magnitude of the level of infection, and the fact that we do have a very serious problem here.

One other view on this is to actually see how the criminal organization behind My Canadian Pharmacy is using this. So we did an analysis over a two-week period of all the spam that was touting the My Canadian Pharmacy crime gang's websites. We saw that they were capable of sending a million and a half spams a day, like the one we saw with the excerpt from The Hobbit, they were using 106,000 bots, the bot network was incredibly spread out, over 3,200 networks and of course there were the large ones like I have listed here, Telephonica D'Espania and others, but we also see bots on other criminal networks, again, very large number of bots, very successful, very easy for them to increase their volumes and try to stay ahead of what the good guys are doing and I think their profits show, unfortunately, how successful they've been.

So, we've talked about the ways that they get this delivered, how they get your email address, how they get the content in your inbox and how they try to have networks of bots to send it. Now let's talk about what they want you to do once they get it in your inbox, and that is to take action.

Lots of actions that I've listed, but today we

are only going to focus at least in the training wheels version on the websites. Wanting you to go to a website, take a look at the products they're offering, and perhaps take advantage of this erection pack Cialis plus Viagra offer, the special this week.

These are the training wheel components which the panel is going to use later to talk about the more advanced things. If you want to host one of these websites, whether it's My Canadian Pharmacy or FTC.gov, you've got to get the website, you've got to register FTC.gov, you have to publish a phone book, a DNS server who tells people how to get to you, how to get to your IP address, you have to publish the records in that phone books that's the DNS server, you have to get the server and run content on it.

Anyone who wants to run a website has to do these components. When we talk about the ways that they attack us, the way that they try to elude it, we'll talk about it in terms of these components and that's why we're emphasizing this a little bit more than we would otherwise.

So, the last example, back to my favorite spam game in the world, My Canadian Pharmacy, I picked one from my random quarantine, I picked the website that it's referring to and this is what I learned, they had

registered a domain called BigMouseTrack.info, a few days ago, they registered at a registrar called 1877namebid.com, and they filled out the who is information to say who they were registering it, as I've shown here.

The only two things I found out interesting about that is that they used a country code that as far as I can tell does not exist, there's no country in the world that has a +68 prefix, and they used an email address to contact them hosted at Dublin.com, which happens to be run by Suresh's organization, which he could comment on.

They also set up DNS servers, and the records that they used, they used actual computers on broadband residential networks. These are bots, to actually host their phone book, to actually host their DNS servers, and they had multiple ones of them for redundancy on the biggest high speed broadband networks in Taiwan, Spain, U.S., Brazil and other places.

The web server itself was running on a Korean broadband server on their IP address, and the web server itself had locations, multiple locations on the Korean Telecom network, and one of the interesting things was the images weren't hosted on that server, they were being pulled from other bots on other broadband servers

around the world.

Now, I think the panel has a lot to say about these techniques, I'm not going to dwell on it, but it gives you a sense for what they're doing. In particular, the My Canadian Pharmacy gang has been integrating over the last 18 months using a number of techniques to stay ahead of the good guys and make it tough to shut them down and to obfuscate what they're doing.

And then I wanted to mention two things and we're not go to focus on them on the panel, there are other panels, but to make sure we understand the full scope, some types of spam, they actually get money directly from the consumer. My Canadian Pharmacy, you give them a Visa card number and they run that credit card and in some cases they actually fulfill the order.

I'm sure a lot of people in law enforcement know about it, but if you place an order from My Canadian Pharmacy, you may get an envelope like this with some pills, you may get one like this with some pills. It may come from China, it may come from India, but in some cases the spammers actually have large-scale sophisticated distribution supply chain organizations that are shipping product, may be legitimate, may not be legitimate, around the world. These are things that are

important to understand because these are the things that we are going to use to expose their weak links and in particular Jon has a lot of expertise in this area which I am looking forward to hearing about. Thank you.

(Applause.)

MR. ST. SAUVER: So, I'm going to go ahead and talk a little bit about the way technology is impacting spam, but also a little bit about the way it's not really all about technology. When I go ahead and say that, what I'm really trying to tell you is that even though we can look at some of the technological evolution that's occurring, it's really also evolving on a business level. It's really also evolving on a strategic level. It's the sort of thing where illegitimate affiliate programs are allowing spammers to scale up their operations in ways that really are fairly amazing. It's also giving us some additional benefits, things like the ability to go ahead and claim that they've advised their affiliates not to spam.

These are the sorts of phenomena that are occurring today that you need to go ahead and be watching for, in addition to things like the evolution of the image spam, in addition to things like the use of botnets.

All of it really comes together in the fact that

we're really seeing the creation of a spam eco system. There's specialization occurring, there are people out there who are niche providers who go ahead and actually serve this particular need. They may harvest addresses, they may go ahead and produce bots, they may write malware. These are all people who are specializing in one particular part of the spam problem and together they form a very powerful consortia. That's the problem that we're facing today.

People are no longer needing to become experts to go ahead and actually spam. They can go out and buy what they need instead of having to build it themselves.

Because that eco system is so complex and vulnerable, it actually is something that can be attacked. Because these people have to go ahead and learn an increasing body of spam trade craft, for example, they need to go ahead and become educated. How do they do it? Well, there are spam forum where they can go ahead and trade notes with their colleagues. We know that they go ahead and are going to need to purchase particular products that will help them go ahead and do their spamming activity. That's going to generate financial records and we'll hear some about how those financial records may be able to be worked.

The problem that we're running into is that

they're scaling up very efficiently and we need to make sure that we're going ahead and doing so as well.

One of the things that is perhaps the biggest spammer vulnerability is the money trail, and the U.S. Money Laundering Threat Assessment Working Group did a really great job of sort of highlighting some of the financial channels that the miscreants are exploiting. In 2005, they went ahead and released the U.S. Money Laundering Threat Assessment, it's the sort of document that I would encourage you all to look at because that really explains how the money is being moved. It's not surprising, given that kind of a document's emergence that they're having fewer and fewer avenues available to use.

For example, we went ahead and learned about a lot of the pill samplers, they are down to one credit card brand that will continue to accept their online pharmacy sales, and if we can go ahead and attack that service provider, that will have a potential impact on the spammers.

I think it's also important to recognize that just as everyone else pays taxes, it's going to be critical that we have the spammers and their affiliates also pay taxes. Talking about Al Capone and the fact that he was eventually busted for income tax evasion,

well, I think we really need to focus on things like income tax liability for some of these affiliate programs. If you have someone signing up anonymously, being paid anonymously, I really sincerely doubt that they're getting a 1099 for their income. So, if they're not going ahead and having these sorts of very basic procedural and administrative things attended to, that perhaps is an avenue that can be used to attack them successfully.

We also heard about the envelopes coming in from overseas containing the pills and so on. Those spams are generating these orders for the pills, they need to get those things to the customers, unless it's actually a case where they're ripping off the customer directly and sometimes that may happen, because after all, who is going to go into the police and say, oh, I'm sorry, I didn't receive the pills I purchased, my Vicodin didn't come in today. No one is going to be willing to admit that.

So, the spammers know that and in some cases they may exploit it, but in other cases they may deliver the honest product. When they do deliver that honest to good product, it's coming in from overseas.

We have borders, in the physical world we do have borders, we don't have borders electronically, but

in the physical world we do. Customs and the Drug Enforcement folks should be able to start interdicting some of those shipments as they come through our borders, unfortunately they may not have the staff that's really needed for them to go ahead and do so.

So, I think we need to look at some of these physical issues, rather than treating it purely as an electronic phenomenon. They do go ahead and have income streams, they do go ahead and have product shipments.

We also know that spammers love anonymity, so as we see things like these financial and fulfillment channels being attacked, we know that the spammers are adapting, and that's why we're seeing increasing levels of things like pump and dump spam or mortgage lead spam, it decouples the spammer from the spam. It decouples the spam from fulfillment channels.

So, we know that there are things that the spammers are relying on to have this sort of anonymity, things like domain name registrations. If you look at these domain name registrations, who does look-ups on them, you will see in many cases they have completely bogus data. We can begin to go ahead and start attacking that channel by looking for those incredibly fraudulent registrations.

There is also the issue of cheap and easy to

create off-shore shell corporations. These, again, are the sort of things that spammers are using to go ahead and provide insulation to go ahead and give them the ability to continue to persist. There are also national privacy laws, particularly in the European Union that really go ahead and make it hard for ISPs and even consumers themselves to take the sort of actions that they would like to go ahead and take to protect themselves.

And I would argue that we still have very primitive methods for international law enforcement cooperation.

One of the things we've heard this morning repeatedly is that spam is an international phenomenon and this really is true. That's one of the messages I hope you take away from this today. Because spam has been mitigated at least in part here in the United States, spammers have responded to that. They have evolved. They have gone ahead and move their operations overseas. Europe in particular has really been badly infested recently.

So, it's the sort of situation where because it is an international phenomenon, it's going to require a coordinated international response. It's not going to help if we clean up all of the America's PCs that may be

infected if we still have millions of infested PCs in Poland, in Turkey, in Spain.

I would also point out that in some cases, we may even be seeing phenomena that have more strategic impact. Spam has really been a central level and has had such a deleterious effect on our economy, it really is a form of low intensity cyber warfare. What a perfect way for those who hate the United States to attack us. We don't even recognize we were being attacked, and if we did, what we would do?

So, I just wanted to leave you with six quick closing thoughts. One is that the Internet really is a giant laboratory for spammers, and they can just try different things and see what works. While we can and have to respond to all those attempts to go ahead and experiment online, we're not going to win if we just continue to play that kind of a defensive ball game. We really need to go on the offense.

Spamming requires a lot of stuff. By that I mean the spammers don't live in their basement, they don't just write all the code they need themselves. They buy things. They go ahead and sell services. There's an eco system out there and that's what we need to attack, is that complex eco system.

There are choke points and those choke points

are the things that we need to go ahead and work on relentlessly. Things like merchant account processing and the interdiction of illegal shipments at our borders are examples of that.

And spamming activity doesn't occur in isolation. There are communication networks out there supporting these spammer activities. We need to go ahead and focus on those, just as we would collect intelligence on a terrorist organization, you need to go ahead and also be prepared to collect intelligence on spam organizations. That needs to be done in a proper way, with all appropriate court approvals and so forth, but we need to go ahead and begin tackling this as a system, as organized crime.

And we also know that the bad guys have done an excellent job of scaling up their operations. If they have thousands, tens of thousands of affiliates, it's going to be hard for us to go ahead and have enough prosecutions to go ahead and deal with all of them. It's great to see people getting busted, I appreciate each and every one of those arrests and prosecutions, but if there are thousands or tens of thousands of spammers, we're just not scaling.

And there's also the problem that spam is an international issue, and one which is going to require

coordinated international effort. We really need to have the United States show leadership in this area, and actually have the same sort of success overseas that we've had in the United States chasing these guys off of what they would like to think of as their safe ground.

And with that, I'll turn it over to Jon.

(Applause.)

MR. PRAED: Good morning, I guess it's still before noon, so good morning. Glad to be here. I am an attorney in private practice, I for the past ten years have largely made our focus the focus of the Internet Law Group to sue fraudsters on behalf of corporate victims. It's not that we don't care about the individual, but quite frankly, the individual as an individual is not going to catch these people. We have to look for ways to leverage our resources and everything that we do has to be focused on how can we act more effectively to get a bigger lever, right? If you have a big enough lever, you can move the world and we have to catch every spammer out there, we just have to look for those leverage opportunities.

The way we sue spammers in the end is by catching them. We track them and identify them through capturing a lot of data. We try to track them across what we call the spam life cycle. I would like to talk

to you today a little bit about some of the observations that we've been able to make over the past ten years of doing this, and provide a little bit of our expertise on what we think are the evolutionary concepts that spammers implement.

At some level, though, I want to say, how are they evolving? To be honest, they're not, in one important way. Spammers do two things, as a result of what we're trying to do, they will always do these two things, and no matter what we do, they will continue to do them. They disperse, and they converge. Everything that we do to them is going to make them react in one of those two ways. I don't care what they're doing, I don't care what we do to them, they will react in one of those two ways.

Everything else is a tactic. The strategy we have to adopt is to focus on how do can we take advantage of their dispersion, how can we take advantage of their convergence, and I think some of the things that we have done through our involvement in some of these civil litigation cases, you will see there are lots of things that we can do if they react in either way.

I don't care, they're going to move one way or the other, the trick is that we have to anticipate and

react to it.

Now, one of the things I would like to do is try to echo some of the questions that Joe has raised, which I think are fantastic questions. I think I have heard lots of speeches on spam, Joe's presentation you just saw is I think one of the most elegant in terms of focusing on the macro solution to the problem. It is a complex problem. We are not fighting mosquitoes as we fought in the Panama Canal, having to build the Panama Canal, we had to address the yellow fever problem. Those mosquitoes didn't have nearly the brain that spammers have. Spammers are extremely intelligent, they react. This is in some sense a world health issue, if you will, in terms of trying to deal with a macro germ, but these are not germs, they're not mosquitoes, they react, and we have to take that into account.

We have a current lawsuit pending that we filed in Federal Court in Virginia that is targeting spammers who are themselves targeting email addresses that they have harvested through websites that their robots are visiting. Our client is an enemy called Project Honeypot, which is a nonprofit organization that provides a distributed network of spam-trapped honeypots that basically install honeypots on websites, any of you today can download one of their honeypots, install it on

your website, and if anyone visits that particular honeypot, they will be handed out a unique email address and their IP address and other characteristics of their web browser will be captured by Project HoneyPot and retained. Then project honey put sits back and waits, and waits, and waits, until that email address receives a response. They've been doing this for the past two and a half years and in the past two and a half years they have received millions of email messages that have been sent from millions of spam harvesters, excuse me, from millions of spam servers.

What's interesting, however, is that the number of harvesters that have collected those millions of email addresses is only in the 19,000 range. 19,000 unique IP addresses have harvested those millions of email addresses to send those millions of spam messages. It's a ratio of 178 spam servers, botnet spam servers for every one harvester out there.

So, in the effort to try to catch these guys, yes, we have to focus on botnets, yes, we have to take it, but the moment you take on that fight, recognize you're fighting an army that's 178 times larger, artificially larger, than the true number of cadets on the other side facing you. There really aren't that many people doing this, and some of the resources that

they use and exploit, specifically the harvester community, is a much smaller, narrower stream that we have to find a way to bridge across in order to get to the other side towards hard identity.

Our lawsuit is targeting those harvesters. We currently have John Doe discovery. One of the things I want to jump into is show you some of the strategy that we use in some of the vulnerabilities that we see in the spam community through the John Doe discovery.

One of the interesting statistics, though, that's come from the Project HoneyPot harvesting information is that most of the visits these honeypots are being made by robots. Many of them are good robots, but not all of them are. Obviously the ones that send spam are bad robots. Of all the visits that they've seen, about eight percent of all visits result in spam, which means eight percent of all robots out there are essentially bad robots. It's a very large community if you take in mind how many people out there are using robots for good on the Internet. Eight percent of that universe is out there for one reason and one reason only, they're looking for your email address because they want to send something to you.

I said earlier, spammers evolve, but they really only react in one of two ways, they disperse or they

converge. One way that I think spam is evolving, and I thank Tom Grasso and the FBI for commenting on it, spam is increasingly going into the criminal arena. It used to be that spammers were kids or entrepreneurs, if you will, trying to make money. They are still there doing this, but most spam today, I submit to you, is not designed to actually engage in any sort of commerce, even illegal commerce, it is quickly running to a pure criminal enterprise. I submit to you at the next FTC spam conference, we will not even be addressing the commercial aspects of this activity, what we're going to see is spam being sent out for three purposes, extortion, terrorism, and warfare, between nation states.

Extortion in the sense that you are going to get an email message that's going to have in it a photograph of your child, and they're going to say, I know who your kid is, I know when he gets dropped off at school and I'm going to kill him on Thursday of next week unless you wire money to this bank account. CNN is going to report that that happened last week, a week later you're going to get that message. What are you going to do?

Terrorism, obviously, we're already seeing links between terrorism and spam and warfare between nation states. I think we are seeing that to a large extent,

to a large extent that simply is not reported.

Eastern Europe, with the break-up of the Soviet Union, we're seeing a lot of activity there take place in the cyber arena, and we as a society have got to deal with how are we going to deal with the Internet if this problem that was a simple, gee, I get a lot of stuff I'm not really interested in buying, converts into extortion, terrorism and traditional cyber warfare.

Now, let me turn to, I'll go back instead of forward. Let me turn to what do we use civil litigation for? Civil litigation is that extremely helpful supplement to the criminal law enforcement process. Largely because, again, leverage. There are a lot more civil litigators and lawyers out there than there are official government law enforcement actors.

One of the things we have to find a way to do is leverage what we as a society can know and can find out about the bad guys by leveraging what we can learn through John Doe civil discovery process. I outline for those of you, if you can read this, the process that we generally follow, the first step obviously is filing the John Doe complaint.

We've done that in our Project Honeypot lawsuit, asked the court for permission to issue subpoenas to various parties, then you issue those subpoenas to the

sources of information. They're largely five sources of information. You have Internet companies that are providing connectivity in one way or another for the websites or the domain names, or the drop sites that are being used. But you have lots of other sources of information that you can go to besides the Internet providers. You have telephone providers, land line providers, cell line providers, as well as IP telephony providers. Spammers need to have access to telephones, and the telco providers are the ones that provide it to them.

You also obviously have financial institutions that are either providing them with banking services, credit cart card processing or sort of nontraditional developing methods of payment. All of those are often subject to subpoena, all of them often operate in a multinational context and are extremely interested in many of the changes that are coming about in law enforcement rules and regulations concerning know your customer rules, in gaining penetrability into knowing more and more about the spammer community.

If you can get a spammer's bank account records, you can get everything that you want to know about that spammer. The John Doe civil litigation process is an excellent way to start that off so that when we hand a

case off to law enforcement, they have an extremely well developed case for prosecution.

Physical address owners can also be subpoenaed. Private mailboxes are frequently used by bad guys, and if you open a private mailbox in the United States, the private mailbox owner is required by law to take a driver's license or other government-issued photo ID. Jeremy James was prosecuted on that, his accomplice, Richard Rakoswki showed his driver's license and that driver's license photograph was copied, God bless him, in North Carolina, and drove all the way up to North Carolina, and explained because of a government agent who asked him to do so, he crawled through his attic and looked through dozens of boxes of photographs of driver's licenses that he had made, because that's what the law required him to do. He was a first generation immigrant, and you have to applaud that sort of citizen soldier who does the right thing and because of it has in his attic a box of paper that has on it the information we need to catch the bad guy and put him away.

Jeremy James, of course, was sentenced to nine years in prison, because of the spam activity. So, physical address owners are an extremely useful resource. Shippers, last of all, are extremely useful,

because most bad guys who are shipping anything, even if it's a fraudulent product, have to have some way to get it there.

So, all five of these sort of areas of discovery are available to us, and each of them in their own way can provide useful information. All of that information then gets reviewed, and analyzed to ask, is there some data point in the response that we have seen that leads to actionable information, can we seize a bank account, can we name and serve someone, put a complaint in their hands that obligates them to appear in a court that has some power over them to put it to them. Or can we give the information to law enforcement who can put handcuffs on these people.

If there is no information that's actionable in that first, we simply rinse and repeat. We get lots of information from subpoenas and we can repeat that process almost endlessly until we find something to catch the bad guy, and ultimately, ultimately they can be caught because they all make a mistake. They all seek anonymity, which is why they disperse or they converge.

They seek to disperse across white hats so that no one of us has the motivation to do anything substantial to stop them or they converge across black

hats because they hope that the black hats will be able to be paid enough to hide their identity.

I submit to you, if you think about the complexity of dealing with those two reactions, we can, within the room, deal with how do we deal with dispersion? We share data amongst ourselves. How do we deal with convergence? We have to find a way, as Joe suggests, to build and enforce borders so that we can keep black hats out of the rest of the network that the rest of us use.

I appreciate the opportunity to be here. Thanks very much.

(Applause.)

MR. HODAPP: Now we would like to have some discussion within our panel and we would like to start with some of the first topics that were raised in Patrick's presentation, which is the email harvesting. In fact, in Jon's lawsuit, he has alleged that Project HoneyPot had 6.1 million spam messages received over 15 months because of the harvesting that he was suing the defendants for. I'm wondering, Suresh, can you address whether this same problem is occurring internationally?

MR. RAMASUBRAMANIAN: Well, chosen techniques are much the same variable that are used and a spammer in China or in Brazil can use the same techniques that a

spammer in United States can. He probably downloads the same set of software or hires the same botnets from the same set of people.

So, spam is truly international, and there's not going to be anything much different about the spam that somebody in China receives compared to the spam that you receive in the United States. It's some local business targeting you with localized spam so that you get Chinese spam in China or you get a local business spam in the United States as well. That's the general pump and dump and stock product stuff.

MR. HODAPP: Suresh, you indicated that one of the ways that people can protect themselves by having their email harvested is having something in place that is not actionable, such as using the word "at" instead of a symbol, or using throw-away email addresses as an additional protection. Do those still work?

MR. RAMASUBRAMANIAN: That used to work ages back, but when you look at a botnet that can mind the contents of an Outlook address book or files on your desktop, well, you're out of luck. If you're looking at web harvesters which do account for a good amount of the traditional person that does this harvesting, yes, that kind of thing will work, but to make it sufficiently unreadable to a bot, you have to make it just as

unreadable or even more unreadable to a human being. No point in that.

MR. HODAPP: If we can discuss briefly, if there's any other methods that be can be used to try and reduce harvesting, I think, Patrick, the one thing that IronPort had mentioned was the possibility of reducing, not bouncing invalid addresses immediately. Can you address that?

MR. PETERSON: Sure. So, there's a lot of vendors who make solutions and there's even lots that plug into open source solutions for email security that attempt, and in some cases are very successful, to protect against the directory harvest attack. So, when they say, JSmith, Jim.Smith, you don't actually just say, yes, they work here, or no, they don't work here, yes, this is a valid address, no, this isn't a valid address.

Without going into the technical details, you basically limit that amount of information and you apply methods so that when you detect someone that seems to be harvesting, you shut down their ability to have that kind of information. So there's vendors on the market that do it, and if you take some of the techniques that you mentioned, if you take those techniques, you definitely can reduce the amount that your email address

is disseminated, but if you have a friend and they've got an Outlook address book with yours and they get infected, that might be one place that it leaks out.

MR. HODAPP: Does that result in this evolution basically resulting in harvesting by one means or another being very effective and very difficult to deal with that? Is that the conclusion of this?

MR. RAMASUBRAMANIAN: Well, you cannot avoid getting your email address harvested. The one thing you can do is be conservative about who you give your email address to, and if you are using your email address somewhere public, like a website or a mailing list or a forum, make sure that you got it through the email address that you use just for that purpose. Free email addresses are downloadable from Hotmail, Gmail and other servers. Use those and learn to keep your information private as far as possible. It certainly won't stop your address from being harvested, but it will minimize or mitigate the risk.

In spam filtering and in trying to stop spam, stop botnets, nobody will claim solution, because no solution exists, any more than there exists a solution for a disease, a pandemic. It's still going to be there, it's going to be a fact of life. So, you follow models that are current in the security and what you

call it, pest control or disease mitigation sectors, where you try to minimize the factors that encourage this from developing.

If you are trying to stop a disease, you drain swamps nearby and you distribute rules to people and you teach them to watch for signs of a disease and do things like that.

MR. HODAPP: So, those are good analyses, Suresh. I think we want to move on and address the second spam requirement. The addresses are one thing, but then they also need to have a subject matter, and Patrick previewed an issue that occurred in one of our discussions that perhaps you could address, Joe, which is the different types of costs and risks that are the choices a spammer makes when they choose the types of products or services to sell.

MR. ST. SAUVER: So, obviously there are going to be some differences in terms of connection between the spam subject matter and the recompense that they receive. So, for example, a mortgage spam might actually result in a larger payback or a larger payment amount than some other spam might. On the other hand, you might have fewer people actually follow through on those.

So, there's sort of the economic equation that

each of the spammers is mentally reviewing. Things like stocks pump and dump spam is so popular these days simply because it allows people to have huge leverage. They can go ahead and make gains that are not going to be attainable if they're promoting some commercial product. I think that might be sort of the area that you're attempting to highlight.

MR. HODAPP: It is, yes. There's the incidence of returns, but there's another factor that perhaps John could address which would be if there's differing legal risks. For example, some of the pharma spam, is there legal risk for some of the pharma spam?

MR. PRAED: Well, certainly you're violating more laws if you're selling product that is more and more illegal and not just illegal, but also is already subject to a fairly robust law enforcement process. I think you see a lot of pharmacy spam today, in fact I know it, three years ago you saw hydrocodone being advertised in the email themselves. That completely disappeared. Two and a half, three years ago, because they realized, whoops, that's the third rail, you're dealing controlled substances openly, there are lots of law enforcement procedures that have been in place for 40 years now, quite well developed, that are going to take you out.

So, you see most pharmacy spam focusing on still prescription drug, but it's much less controlled substances. Pump and dump is the same way. It's much easier to get away with the money when you don't have to tell your victim to go to some tree where you've got their kid that you've kidnapped waiting to exchange for the bag of money. Pump and dump, you get someone to buy, you've already bought previously, or sold short, and you don't have to have an individualized transaction with the victim that is initiated through the spam. It's a separate transaction, if you will. It makes them much harder to catch.

MR. HODAPP: Looking at it from the point of view of both spam and malware, using these bots for one or the other, which I guess you can do either, Suresh, you mentioned, I think, that the spam was pretty much the same internationally. Is that true, also, of the other techniques that the malware type of spam, the malware operators will use, is it the same as a DDoS attacks, for example?

MR. RAMASUBRAMANIAN: Well, yes. A lot of the malware economy is highly centralized. You've got a very small subset of people that actually write the malware and you've got a small subset of people who create and rent out botnets. You have a completely

diverse customer base for those.

For example, right now, the Nigerian spammers who used to be creative and use email to tell the world about hidden treasure are blind lists of compromised accounts on U.S. cable modem providers, Roadrunner, Adelphia, places like that, and they are scamming through those stolen accounts. The accounts that are stolen are also accompanied by ID theft and the guy's credit card information is gone as well and then he finds his email address being used to send out these scams.

So, the botnet economy is truly international, there's no borders there, and any borders that do exist, exist only in terms of the physical transaction, if any. Like for example, there's no physical transaction required now for stealing somebody's credit card, or trying to pump up the value of a stock.

There is transaction required for trying to convince the guy to buy a market share or buy pills online and things like that. So, that's the thing you have to take into account, and the tools and the techniques are completely universal, they're not going to be different as such. The difference you will get internationally is that different countries have different sets of laws and different sets of

competencies in dealing with spam, so that if you have a country with a weak legal regime which doesn't have appropriate laws to deal with the issue, and where the ISPs are a few generations behind in filtering, then that country has got problems.

MR. HODAPP: Thank you, Suresh. I would like to move to one of the major areas for this panel, which is the use of the bots, the dissemination of the message, Ben, as director for network abuse for GoDaddy, Patrick had mentioned that there were some other methods that he didn't focus on for distributing spam, such as web servers, or web forums. Could you address that, please.

MR. BUTLER: Yes. You know, we've talked about bots being a situation where they've taken over home PCs, personal computers, and are using those to send out the spam. One of the I guess areas that we can get a little success in dealing with PC-based bots is that ISPs can filter on specific ports to try and limit outgoing email and channel it through their legitimate mail server, thereby being able to apply outbound filtering and so forth, but what they have begun to do now is they have begun to take over web servers and websites that belong to legitimate companies, legitimate web hosting customers, because those servers don't have the same restrictions.

For example, think of any random website that you might go to, and they have a contact us forum on their website, it's a script that you can send feedback to the site over. That feedback goes in the method of email and when they can take over a web server, they can use that same permission to send email that the contact forum is designed for and instead send whatever they inject in there to whomever they decide.

So, web servers have become a major problem. It's the same basic philosophy as a botnet, they get in through script vulnerabilities, weak passwords, things like that, but when they do that, they also create another barrier to try and keep it more difficult for someone to actually track down the spammer involved.

Abuse staff, for example, has to spend their time in customer education efforts with the legitimate customer, to help them understand how secure their bots, rather than being able to spend all their time chasing down the actual bad guys. So, it's definitely another head on the same dragon.

MR. HODAPP: What kind of success has GoDaddy had in addressing that problem?

MR. BUTLER: Well, I mean, I'm not going to lie to you and tell you we've found the ultimate solution. Obviously one of the major components is customer

education, are legitimate hosting customers have to be made aware of the seriousness of the responsibility they're taking on when they get, say, a dedicated server. They need to be aware that they have to keep their scripts and their server-side software up to date to try with security patches and that sort of thing.

The other thing that we can do is we've, even with our dedicated servers, we filter all email through our own relay system so that we can apply outbound filtering. Not all hosting providers are able to do that at this point. So, the same types of things that protect you from getting it into your bulk mail versus your inbox can be applied outbound by your ISPs, and hopefully cut down the amount that's actually tracked.

MR. HODAPP: In addition to the things to prevent the outbound dissemination of web pages that have malware, can some other panelists mention some things that could be done at the ISP level to prevent that from coming in? Are there solutions at the recipient level?

MR. PETERSON: For the web-based?

MR. HODAPP: Yes.

MR. PETERSON: There are some solutions, but I have to say that I am quite pessimistic on this. So, people receive things in email from time to time and

they become infected or they can be accessed offer the Internet with the network vulnerability. When it comes to the web, people are so used to clicking on bright, shiny things, free things, screen savers, accelerate your bandwidth, new plug-ins, and they are so used to downloading that new version of Shockwave or that new version of the toolbar, that it's really, really easier for criminals to convince them that there's some other neat, new shiny thing, which may in fact be giving them the screen saver, but also giving them some form of malware.

So, there are Internet companies that are providing web-based security, not just the email, there are some ISPs that are providing value-added services based upon protecting them around the web. But it's a very challenging area because it lends itself to criminals doing social engineering, because people are trained and so used to downloading and clicking on things over the web.

MR. HODAPP: Would this be a place where you might apply reputation-based analysis and filter more vigorously on something coming from let's say the back alley website, a bad neighborhood website?

MR. PETERSON: That's a great segue into a point I wanted to make and we've seen many technology vendors,

three or four years ago they said, we have this thing for reputation, we can tell the difference between a bot and a legitimate server, now a lot of those companies are saying we have that same reputational concept for the web. We know the difference between a good server, GoDaddy, and some name that's been registered and hosted on some kind of overseas provider who does bad things, and we know that people shouldn't be going to that server because it has attributes which are very much like a bad server.

And I think this is a new frontier that's really important for us to attack. Five years ago if you had said to a lot of the providers here, hey, you've got people on your network who are sending spam, I think a lot of them would have said, they're paying me for a service to access the Internet, I can't restrict them from doing that.

Now if you talk to any of them, they are absolutely, we know the problem, we know we have a responsibility. I think unfortunately today, GoDaddy is a bit of a minority of saying we're a web-hosting provider, we're a domain name registrar, it's our job to police our customers, it's our job to spend our money and our time to basically keep our web infrastructure and the domains that we use used for good.

Unfortunately, there are 699 other registrars who don't and haven't been fighting the issue and I think the bad guys are leveraging them and I think that's a problem which is going to take a while to be educated on and that means the bad guys are going to go after it very aggressively.

MR. RAMASUBRAMANIAN: Yes, I would like to add only one thing to it. A lot of the problem here is that we get plenty of people in the same room and talking the same things, they are taking the same measures. Unfortunately, this just means that spammers are people who distribute malware or launch D-DOS attacks, will go to the registrars and will go to the countries and will go to the ISPs that don't do this. You still have to deal with them because those registrars, those countries, those ISPs have lots of legitimate users as well.

Simply blocking them may not always be practical, in fact, in 99.99 percent of cases of broad-based blocking, it's never that practical. So, the one thing we have to do is engage them and there are several international initiatives that try to do that, with a small amount of success. The problem is that we can't wait for those economies or those ISPs to come to us and say what can we do? We have to go to them, we'll

have to use the contacts we have in those countries or those ISPs to do things. I think a subsequent panel will be discussing that a lot, so I'll stop right there.

MR. HODAPP: Okay. We had focused, Patrick had focused on four of the spamming requirements, and the fourth one was the action for recipients, which has produced some other problems, I believe, and Joe, could you mention the one in particular that's involved with the hosting of messing with DNS and the hosting? Thank you.

MR. ST. SAUVER: So, I think what you're alluding to actually is the problem of fast flux hosting, so that if you think about the spammers, they want to go ahead and host their web pages somewhere. Legitimate hosting companies want to see those spammer pages. When they get complaints about those spammer pages, they take the spammer pages down. So, just like any other business, the spammer basically faces a real problem, they want to have a stable, reliably available website that they can point customers at. Well, legitimate hosting companies won't allow them to do that.

So, what spammers have done now is they've said, well, I've got millions of bots out there, millions of compromised hosts, I can use some of them to host web

pages. Now, they don't want to have a single host used for that purpose, they want to have multiple hosts used at the same time. So, if any one host gets turned off, if any one host gets cleaned up or blocked, they're still online. That problem of fast flux hosting is going to become increasingly difficult over time and it's going to be crucial that the registration service providers, the registrars all kind of chip in to go ahead and start attacking that, because this is only going to be able to be attacked at that level.

The thing that you are going to run into more and more is spammers are going to start using all these zombie machines for things other than sending spam. Denial of service attacks, we've already seen them using them for that purpose. We know that they're now hosting their DNS service on that. They've basically recognized that they have a very fungible and malleable type of product that they can use for a variety of different purposes.

So, these bots, even if you go ahead and block them from sending spam on port 25, they can still be used for a phenomenal number of other purposes, including hosting web pages. When they begin to go ahead and do that, you lose the ability to go ahead and tear them down. It becomes a lot harder to go ahead and

attack those sorts of hosts.

So, that's an issue that's emerging. We know that there are things that can be done to go ahead and begin to deal with that, in part at the DNS level, in part at the registrar, registry, registration service provider level, but it's an issue that I am not sure has received a lot of attention to date.

MR. PETERSON: Just more elaboration. You know, for an example of what Joe is saying, they've hosted a bad site at GoDaddy, I give Ben a call, he takes it down, they've got to go set up another one, it costs them money, it costs them time. We find another domain, like the one I gave the example of earlier, they can extract info from My Canadian Pharmacy, I say, ah-hah, it's being hosted on somebody's PC on the Comcast Network, so I give Michael O'Riordan a call and he takes it down.

And then I check the phone book again, the DNS record, and it's pointing somewhere else. The exact same domain is now pointing somewhere else. So I give somebody else a call, and they could basically point to where that domain goes to lots and lots of different zombies, so as now, whereas before with one phone call, hypothetically speaking, or one block of that, it was effective, now they're doing the fast flux and they're

moving it all over their bot network.

MR. HODAPP: How fast are we seeing them change the location of the DNS servers or the websites?

MR. ST. SAUVER: A lot of times the TTLs or time to live is 60 seconds, so they could literally go in and change it on a moment's notice.

MR. RAMASUBRAMANIAN: And the registrars are right now the only single point of failure in this model if you use a domain name, and quite a lot of them currently do.

MR. HODAPP: And that has been done, actually, GoDaddy has done that, haven't they, Ben?

MR. RAMASUBRAMANIAN: GoDaddy isn't, as somebody else pointed out, the only registrar in the market. There are other registrars who are perfectly happy to take a spammer's money or a malware writer's money and register it. There are other registrars who may not be aware that these are spam or malware domains and they might not have tools or techniques or capacity in place to deal with these issues.

So, it is either ignorance or a whole bunch of shades in between. But yeah, GoDaddy is not the only provider in the area where you can get a domain from. Unfortunately.

MR. BUTLER: The thing with domain names as a

single point of failure for taking down spam operations, it's been that way for a long time, whether they leave the domain name pointed to a particular host for a week or a month or a day or 60 seconds. We are working extremely vigorously within the IT field, the IT field and the governing body for registrars in trying to encourage our competitors to do the same thing. We don't want to have a monopoly on taking down spam domain names. It doesn't do the community, the Internet at large, any good, if only one person does this, as Suresh pointed out.

Fast flux is a slightly more involved method that's coming along, and we see it as just another opportunity to identify who the real bad operators are. I can take down a spam website for a guy who maybe just didn't realize that he couldn't buy an email address list and start sending out emails. He can be educated, that behavior can be corrected, but the bad operators who are using fast flux, these are the guys that we really want to identify and go after even more vigorously.

So, it's another tool in the tool belt essentially.

MR. HODAPP: Ben, that was --

MR. RAMASUBRAMANIAN: There's one thing, though.

A domain registrar's actions are quite often as much of a force multiplier in this game as botnets are. When you've got one guy who is able to command several hundred thousand bot accesses, quite often he will go and register 200 or 300 domains with the same provider. When you know that there is a fraudulent domain and he's got 300 other domains just like that, you can take the whole lot down and that's going to cut that back quite a lot.

MR. HODAPP: Actually, Ben, your question is a good question and answer from the audience. There is from the last panel one written question that I think reflects that and I would like to have anyone who feels they can respond to this. The question was, is it more common to see legitimate senders sending high volume mail from a single or few recognized IP addresses versus a botnet that sends a few messages across a distributed set of consumers' IP addresses?

MR. BUTLER: Yes.

MR. HODAPP: So, in a way --

MR. BUTLER: They all have their own methods that they choose. I mean, we're focusing on the botnets and the very hard core relatively small group of people that's responsible for a bulk of the spam, but all these new tactics that we're talking about aren't replacing

the old ones. They aren't replacing the misguided email marketer who just doesn't understand the need for confirmed permission. Spam in its old form still exists. We're just trying to focus on what's going to give us the biggest victory with this particular summit.

MR. RAMASUBRAMANIAN: Well, for a provider, spam is spam, and when your users are clicking to report a spam, they will report faulty emails from a static service provider which generates a high number of complaints, just like they will report those spams sent from a botnet. Your job as a provider is to integrate all those reports into something useful, and quite often you will find that spam is spam, whether it's sent from a botnet or whether it's sent from a hosting facility, a dedicated hosting facility, the result is the same for your users, it's spam.

Of course, the spam might be rather less fraudulent and it just might be unsolicited marketing, but in the interest of it's one piece of email versus some other piece of email as far as an ISP is concerned.

MR. HODAPP: There is another question written out that concerns remediation or prevention, and this is a question of whether web hosting occurs over a particular port, and if so, whether a consumer's firewall program can block that port. Could someone

address that?

MR. RAMASUBRAMANIAN: Joe?

MR. ST. SAUVER: Well, if you go ahead and think about it, normally web traffic happens on port eight, so obviously that is something that could indeed be blocked. However, what we have also seen is spammers go ahead and host web services on any arbitrary port. So, if you ever see a URL that says, some web address, colon, and a port number, that's a very obvious way that they can go ahead and get around any kind of filtering that's done on a per port basis.

MR. HODAPP: So, when they have a spam message that has a domain name in it, and they're relying on fast flux to give them a different IP address, they could direct it to a different port than port 80 to prevent that?

MR. ST. SAUVER: That would potentially be another strategy they could employ, sure.

MR. PETERSON: If I wasn't running a web server, I could say don't let port 80 in, because I don't have a web server, and then they would say, oh, if they infected my PC, let's run some software and have it access the web over port 25 or port 22, and if I didn't block those, they could actually get to it kind of in a sophisticated technique.

MR. RAMASUBRAMANIAN: Or if it's malware filtering that you have on the PC end, it can always be undone or reversed.

MR. HODAPP: Let's get another question. Steve? Steve Baker, the regional director for our midwest regional office.

MR. BAKER: One question we've got to ask ourselves as law enforcers is why this matters. In other words, what's the consumer injury? We've heard the Pew woman say that 95 percent of people say this is a nuisance, we can live with it, and a lot of people are saying that 95 percent of the email out there, you guys have identified as spam. Model law enforcers are used to usually having somebody sell diet pills and then they sell a half million dollars worth of those, consumers pay a half million, the bad guy gets a half million, so your consumer injury is equal to what consumers spend, but I wonder if there are system cost is here where a spammer who makes a half a million dollars is costing all of us collectively more than the amount that he takes from consumers. Or whether the costs are really -- the filters and stuff are so low that the consumer injury is really what consumers are losing.

MR. PRAED: We're not going to cure AIDS as fast as we would otherwise because drug companies are not

recouping the cost of discovering new elements because they can't sell the real stuff because somebody out there is manufacturing counterfeit stuff out of some lab in some basement in India or China, and he's selling that at a third of the cost of what the legitimate stuff can be bought for.

Real people are drying from taking those pills, and real people are dying because profit can't be put back into research and development to find new drugs that are going to save us from things that are killing us every day or they're going to start killing us tomorrow. That's just in the pharmacy arena.

MR. RAMASUBRAMANIAN: Let's put it this way: Spam is a philandering crime and it's a fraction of a cent from somebody and a fraction of a cent from somebody else and pretty soon you're talking real money, but the generic drugs are doing it as well. You've got quite a lot of legitimate companies in India and China are manufacturing junk pills and you've got licenses of drugs from those manufacturers, reputed alleged people and selling those for a fraction of a cost for what did it take to buy those from a mainstream manufacturer in the U.S. or Switzerland, but the stuff that's being sold by the underground economy is typically things that are manufactured in underground labs or in facilities with

poor manufacturing tolerances, or, for example, they might be stealth production runs, sneak into the plant at night and bribe the foreman to run the pill making machines for a little more and nobody is the wiser. Things like that. That is what would typically cause the loss of life or loss of health in pill spam that you are getting when you buy anonymous pills off the Internet.

MR. HODAPP: Okay, Suresh, let's see if we can get a couple of more questions. The gentleman in the back there.

MS. FOX: Jeff Fox from Consumer Reports. I have two questions related to the use of PCs as bots. One, do we know how many PC-based bots are within the United States versus outside of the United States, because if most of them are outside the U.S., all our efforts to educate American consumers are not going to really have much of an impact.

The second question is, it seems to me that the behavior of a home-based PC as a bot, the behavior ought to be quite different than normal everyday activities that most consumers engage in. So, if my home computer begins spewing email or a distributed denial of service attack, perhaps at 3:00 in the morning or when not running my email program, shouldn't it be possible for

client software, including firewalls, anti-malware or the operating system, by behavioral patterns, to be able to recognize this and stop it at the client?

MR. PETERSON: So, great question --

MR. RAMASUBRAMANIAN: Can I take some of that, if you don't mind?

MR. PETERSON: Let me jump in first. The first question is yes, unfortunately, the majority of bots today are outside the U.S. There's lots of figures, but I'm sure that no more than 20 or 30 percent of all the worldwide bots, perhaps less now, are outside the U.S. so, certainly we should not not educate U.S. consumers, but that's not going to solve the problem.

On the second question, there are definitely things which bots, even smart ones, the ones who have gone to university, and cooking what they're doing, or doing, which can be detected, either by your local security solution, your anti-virus or your firewall, and lots of products do that today, and by your ISP. ISPs are deploying techniques more and more to identify things which are anomalous and to either alert the consumer or to stop it from happening. Again, unfortunately it's a boil the ocean problem. People have to install that software, understand it, configure it, but those things are happening today.

MR. RAMASUBRAMANIAN: And if I may point out, the reason why you've got rather fewer bots in the U.S. is because the U.S. has, at least according to some figures I saw, less broadband collectively than Estonia has in its own country. When you can get broadband for very cheap, $30, $40 for a 50 meg broadband pipes in countries, and if you also have a problem that you can buy copies of Windows XP for cheaper than a coffee at Starbuck's, in those countries, well, the bot problem is going to be much more severe there. Even when you have a provider there who is not aware of how best to fix a bot problem.

MR. HODAPP: Thank you, Suresh, and thank you for the panel. I found it very informative, and we appreciate all the work you've done. So, thank you.

(Applause.)

MR. HODAPP: I would like to remind you you are on your own now, and what time? 1:45 is the next panel.

(Whereupon, at 12:35 p.m., a lunch recess was taken.)

AFTERNOON SESSION

(1:45 p.m.)

UNCOVERING THE MALWARE ECONOMY

MS. DREXLER: Welcome back, everyone. Hope you all didn't get too wet out there during that afternoon lunch storm we just had. My name is Sheryl Drexler, I'm an investigator in our Division of Marketing Practices, and I was also involved with the 2003 spam forum that we've heard quite a bit about today, and one of the things in the 2003 spam forum was a panel on the economics of spam, and we're going to talk about that in just a minute, but I just want to first remind you all to please silence any of your devices that you have on you, and if I can remind the panelists please to speak into the microphones or the webcast will not hear you. Also, feel free to fill out those question cards that you have, we will use those during the Q&A session at the end.

And so, without further ado, we will move on to this panel. In 2003, as I was saying, we had the Spam Forum, economics of spam panel, and this panel was very different than what we're going to be talking about today. That panel dealt more with what makes a good email marketing campaign, it talked about why we should be using email as opposed to regular traditional snail

mail. It really focused more on why we're using email marketing.

This panel is going to have a very different focus. We're going to be talking more about these technological tools that we heard so much about in the last panel before lunch. We're going to be talking about why the cybercriminals use these tools. We're going to be talking about what the incentives are.

We're also going to be talking about the cost along the email chain to both mainly small businesses, as well as consumers and other interested parties, and one thing that you're going to notice in this panel is we have a definite theme is going to emerge.

Previously, email was more about the idea of sending an unsolicited commercial email, and we're talking about spam, it's this unsolicited commercial email that was touting a product. Now we're going to be talking about this shift in we heard Tom Grasso in the first panel and others talk about.

We're talking about malicious spam here. We're talking about messages that are phishing messages. We're talking about other messages where the idea is for spammers to exchange data, whether it's credit card information, or underground tools that they're using, the bots, we heard a little bit about the sale of bots,

so we are going to be going into all these different tools in this panel, and talking about that shift, and I want to you keep in mind that idea of the exchange of data and the exchange of the tools that we're using in order to have these cybercriminals make money.

So, I am going to introduce to you our panel. First we have Andrew Klein, and Andrew is the senior product manager of SonicWALL and he has extensive experience regarding the malware economy and he plans to give us an overview by addressing some of these tools of the trade and how the cybercriminals actually make money with them.

Then we're going to hear from Jens Hinrichsen of RSA, the security division of EMC, and Jens is the product marketing manager for customer solutions, and he's going to talk about phishing and crimeware and show us an example of the damage that's actually done by a malicious financial Trojan that's sent via email and he also has some data on phishing that was another thing in the first panel we talked about some of the data, the hard core seeing what exactly is happening in this arena.

And then we're going to have Greg Crabb, Gregory Crabb, who is a postal inspector, and he is the manager for the Postal Inspection Service's Global

Investigations Division. He's going to talk about some of the places that the cybercriminals exchange the data that they have gleaned from this malicious spam and these other tools and where they're exchanged.

Last but not least on the end we have Heinan Landa who is the founder and CEO of Optimal Networks, and they deliver technological and business expertise in the computer network support services arena to both small and mid-sized organizations throughout Washington, D.C., and he's going to talk a little bit more about the financial and physical impacts and productivity costs of spam on especially the small business community.

And, so, I'm going to turn it over now to Andy.

MR. KLEIN: Thank you, Sheryl. How are you? How's everybody today? I hope you had a good lunch. Let's see if we can get this going.

So, I started out in this business several years ago actually trying to get spam, that was my first job, in the whole email security arena. What it caused me to do was to begin to think like a spammer, how would I want to try to reach people. That's an interesting perspective when you get on that side of things.

The next thing that kind of came along was phishing, phishing came along a couple of years later, it's been out there for four or five years in some way,

shape or form, and what happened there was the game started to change a little bit, the economics started to change a little bit, and one of the things that I started to see was a little bit more organization around the efforts, and we've heard some of that already today. What I did was put together this model, and this is a fairly high level model of what I think the economy kind of looks like. Now, on the outside there is those spammers and those phishers who are trying to do what? Trying to make money. It's as simple as that, and they need to construct a tax and construct a tax and launch them and actually collect information.

Now, they used to do that all by themselves, right, a very simple thing to do and at one point they tried to collect everything and tried to turn that into cash. They could turn it into cash in any number of different ways, right? They could just use credit card numbers and sell them through some type of a chat room and sell them for ten cents or a dollar or something like that, potentially they could use the credit cards themselves for false transactions.

All kinds of different ways that they could try and turn that into cash, but other information started to show up as well. Account information, for example, log-ins and passwords, and they had no particular thing

to do with those. But they kind of kept them around.

That outside circle worked for a while. But what was starting to happen was, the inside. That whole malware community, which has been around for years, they talked about it this morning, it's all of these folks in their basement and living in their mom's basement for a number of years writing code, doing nefarious types of things. But what started to happen was that code started to become organized. People started to talk to each other. They started to trade back and forth that information. Let me kind of go through some of those examples.

So, the first thing we talked about today, and it's been talked about on a couple of different panels, is botnets, right? One of the tools of the trade is botnets. All right, they send out lots of spam, lots of ways to compromise a machine so that I can use that machine for whatever the purpose I want to use it for, whether it's sending out spam or phishing or something like that, whether I need to store images on there, so on and so forth. There have been examples over the years where people have done that.

For example, Mr. X, he was a Dutch spammer, he's in jail now, by the way, and he had created his own little botnet, 600 or 700 machines which he continually

replenished and he used those to send out spam messages. So, you could create your own. Or, if you weren't that industrious, you could go rent time on one, and here's the typical or a couple of examples here.

You could get from about $300 to about $700 an hour, renting time on a botnet. Now, what does that get you? I have an attack and I want to launch an attack and I need to send out 25 million spam messages. I could do that in a couple of hours, $600, $1,000, whatever the cost may be. That's my cost to start that ball rolling, right? The example there, both of these, by the way, have both been caught, and in parentheses, that 19, is their age, all right? That's what they're doing these days, and by the way, you can see the kind of money they were making, and both of them got caught not because they got caught, but because they got turned in. Why were they driving a Ferrari with no visible means of support? It was that kind of thing.

So, they're somewhat part of a community which allows them to create these things and sell them, all right, but there's no mass organization. There's no building where all of these guys go to work in the morning. All right?

So, but they still work together. The question also came up about how many compromised machines out

there, and the estimates have been a little all over the board. The low I've seen is like 49 million out of an article in USA Today, 70 million from Trend Micro as you can see there, and Venserve, okay, estimates it at well over 100 million. I don't care what number you want to choose, that's a lot of machines. So, when the FBI says they're going to contact a million people, okay, that's scratching the surface.

Now, I applaud their efforts, by the way, because I think that's an excellent thing to do to bring this whole subject up, and get it distributed out and let people know what's going on, there's still a whole lot more work to do.

There's other tricks that we've seen out there. Domains, and we've had a couple of folks on the panel beforehand that were on there and dealing with domains and domain registrations, all right? All of those that are listed there on the left-hand side, all right, all of those were active phishing domains when we got there. All of them. By the way, that's just a short list, some of my favorites. The list can go on and on and on and on. All of them, by the way, are highly confusing to potentially end users. Secure-ebay.com. That could pretty easily fool somebody.

By the way, most end users, great survey, if you

want to run it some time, what's the difference between a .com, a .net, a .info, a .US, a .org, okay, whatever, as it relates to the businesses you're dealing with? Most users can't distinguish that. So that's what the confusion is out in the marketplace with the people that we deal with on a regular basis.

Some of my favorite ones that have happened over the years as it relates to things like domains, Experion issued that as a self certificate, citybank.de.

By the way, that's not the only that happened, but a phisher was able to get an SSL certificate so that when you went to a site, it was actually secure, you could give away your information in a secure environment. All right.

So, but what this all points out is how hard it is for these organizations to monitor and maintain that. That came up this morning, too, you heard the guy at GoDaddy say, we're doing lots of hard things, all right, and they paying $3.99 per year may not be the right thing to do, okay? Maybe we should pay them $4.99 and dedicate that other buck to security or something like that, but that's the game they're in.

They're in a highly competitive space, and the thing that goes first is security. Things like checking the registrar records when somebody registered. I've

seen domains registered to Bugs Bunny, okay, Don Corleone, I've seen one registered that went the following, I need to type something into these fields, return, because if I don't, return, it will be suspicious. That's the kind of thing that could be put into a record. All right?

Other tools of the trade. I bring these up because these are all banks that have been hacked in one way, shape or form or another to host phishing sites. All right? One was a direct bank, it was a bank in China about a year or so ago that was hacked and was hosting ebay sites. So, the reason is that there's people out there that do this for a living, all right?

There's another one that provided a service, so the bank itself actually didn't host its own website, it went to a service to do all of that, and actually run all of those kind of transactions for it. That service got hacked, and subsequently all of the sites got hacked. Okay? Or not all of them, they couldn't get through all of them before it was discovered.

And then even hosting services, so I want to run my own stuff, but I don't run my own servers, I run them somewhere else. Any time, okay, you are running an institution like that, okay, good-old-fashioned, tried and true methods of hacking your machine still work.

All right? Why do you get corporate phishing? Why do people send phishing emails to companies, to get credit card numbers from your employees? Well, that's one of them. But there's also things like your log-in is going to expire on your Outlook account, you need to redo it kind of phishing attacks. Well, what are they really looking for there? They're looking for a way to access your network, so they can use your machine for some of the things that they were talking about in the earlier panel. All right?

So, there's lots of different ways, reasons that they need to get into machines. What's happened is that people are starting to make money with these things. So, here's a spyware kit for sale, $17, and it comes with technical support. You can't get that from Microsoft. Or any other company. My company, included. All right, for $17, you can buy a spyware kit.

Think about that. Somebody invented it, put it for sale, and sold it. Then is offering to support it.

Earlier this year, there was the Panda Virus, I think back in the February time frame. Panda was a virus that a student created and then sold about to 120 different people at $100 a throw. Now, there's two bad things about that. One is there were 120 different people that wanted to buy this, okay, and two, they

could buy it. The Panda Virus was written in a way that he actually gave his source code and everything and you could actually manipulate it so you could create variants of it so it couldn't be caught. That's a very typical strategy now, viruses mutate almost instantaneously out there.

But it goes show that people are beginning to not only create tools and sell it, but they're selling the pieces of them for money. That creates that second level of the economy.

On of the things that Jens will talk about shortly as far as phishing, but there's this notion now of phishing kits. Now these have been around for years, but the breadth is really impressive. You have a product portfolio of as little as $30 up to $3,000, with all kinds of great capabilities in between. You can just imagine a big checklist that says here's all of the great features you get in this one and you get these extra features in this one and you pay more and you get this and this and this, just like a regular product. You can go to sites and find those kinds of evaluations.

I like the one here, there was a little variant that was done to improve phishing kits that you incorporated what's called a universal man-in-the-middle phishing kit, but it was a new technique that was out

there, and it was introduced as part of a phishing kit, and it allowed the phishers to do some things they couldn't do before, and the quote that came, from Guy Narrise [phonetic], by the way, is that it offers a much better return on investment.

We're talking about these things in terms of regular business software. I would love to be able to write software that somebody writes that about. Right? That's what you strive for. I want a big product portfolio, that lots of different people can buy so I can satisfy lots of needs, right, that provides what? A really great return on investment. That's where they are today. That's where these folks in the middle are, in creating these tools, sharing them amongst themselves, right, not only the tools themselves, like phishing kits, but all of the infrastructure pieces underneath. Virus, right? Botnets and so on. All of that moving around in that economy.

So, what I'm going to do now is I will introduce Jens and have him talk a little bit more about phishing as one of the drivers about it, he's got some really cool slides, as she mentioned, about an attack. So, thank you very much.

(Applause.)

MR. HINRICHSEN: Good afternoon, everybody, I'm

going to apologize in advance for my croaky throat. So, if I change pitch a couple of times, it's just my cold at fault.

In any event, thanks again, everybody. Just as some background, I work within what's called our Online Threats Managed Services Group, I know that's quite a mouthful, but we're really focused on everything external threats related, namely phishing, crimeware/Trojans, as well as from an intelligence perspective, and really much of what Andrew was describing before, the sophistication, the demarcation, the level of really specialization in the underground economy across tools, across how the fraudsters communicate, exchange monies and whatnot.

A few of you have seen a couple of these slides that I have used at a couple of presentations before, but I think they underscore an important point as to the relationship between consumers and institutions. Really what obviously the imperative is from the industry perspective, about what's at stake here from trust, from usability, and really return behavior from the entire online channel.

This might be a little bit of an eye chart, but we do a consumer study, we obviously have feedback both obviously qualitative and quantitative from our entire

customer base worldwide, but we want to make sure that we're capturing end user feedback, like you or I as we navigate the web, we use the web, we do online banking, we use our credit card for certain e-commerce purchases.

Two key things: The first in the light blue background says, "Are you less likely to respond to an email from your bank because of the phishing phenomenon?" And clearly, you can see about half are, that shouldn't be a surprise, so that's just kind of a level-setting statistic. The more pointed statistic in terms of really how it impacts the economy, and I think the trend here is interesting, year over year, the other question in white says, "Are you less likely to sign up or continue to use your bank's online services because of the phishing phenomenon?" And this is just couched within phishing. This is not, obviously, the emerging and rapidly emerging crimeware or broader malware space.

So, what we saw here a couple of years ago was 17 percent of users said they were much less likely to use their bank's online services. Again, I know this is couched within financial institutions, but obviously it relates to other industries.

Then we fast forward a year and we go to '05 and it's an encouraging trend. Basically more than half of an improvement to just seven percent of users saying,

gosh, you know what, because of phishing, I'm more leery and I'm not going to use online services because of that.

Now, interesting, though, then when you fast forward a year again to the end of last year, that number jumps right back up again. Really, the supposition here is that the collective ground swell of concern about all of the threats that encompass a user experience in their online experience, whether it's the crimeware or whether it's spyware, ad ware, ransom, or all the wares that are out there, there is certainly an impact on customer comments.

Phishing, whether you get down the stream of what role education plays, certainly it goes up to a point. I think a lot of folks were basically saying, I'm more used to this, I get phish emails a lot, I either ignore them or delete them. That's all great, when we think of how that breaks down in terms of the crimeware economy, I think the key point that's been already touched on today is that blurring or that blending.

Phishing, crimeware, malware, and really that tandem use of fraudsters for social engineering and infecting users with whether it's a botting form of malware or whether it's a multipurpose piece of malware

that's not only going to bot their machine but also has very specified crimeware. Crimeware again being either identity theft or session hijacking to actually ultimately take out funds and transfer funds out of an account.

So, again, from a consumer's perspective, there's still a certain level of trepidation that exists. The key point that I want to talk away here, and I do apologize, when we had submitted these, we didn't have our most recent monthly data. We're seeing, again, about 200 unique institutions that have been targeted on a worldwide level that are being targeted by phishing.

The key point here is not so much the number of institutions by month, and I didn't even bother to put up the number of unique attacks, because certainly given some of the forces at play here, whether it be rock and others, depending on how you count it, it can be possibly misleading, but the key take-away here, if you fast forward to just last month, so I apologize it's not in the chart, but in June, of around the 200 institutions targeted just by what we call classical phishing, nearly 35 had never been attacked before. Thirty-five. It's a staggering number.

So, when we think about this fear of phishing,

phishing is not going away anywhere soon. We keep raising the point as well about ROI, it's darn easy. One of the recent discoveries of our team, and Andy described it best, when you look at the spectrum of just phishing kits that are out there, whether it's really sophisticated phishing-based man-in-the-middle kits or your original kind of static HTML kit, we discovered another interesting other revolution to bring, the newby fraudster with a plug-and-play phishing kit.

Instead of having to go in and insert different files into different folders on a compromised server, within a double click, just as you would install any other software, a newby fraudster or even a fraudster who wants to become more efficient and launch an attack, within two seconds, two seconds an entire phishing attack is ready to go.

That's a pretty staggering improvement when you think about just ease of use and productivity and when you continue to use these economic terms within the fraudster economy.

So, of those 35 institutions that we had never seen attacks against before, about a dozen of them, if we think just from a U.S. perspective, about a dozen were federal credit unions. That's another point. I mean, we have certainly seen for many, many months now,

a transition, actually years, I should take that back, to transition to well beyond the financial sector.

So, it's targeting any kind of institution that has valuable credentials to be had, or gets a lot of traffic. If there's the cover story there to lure somebody using what might be considered either a spam email or as a phish email, but if it's a cover story that's nebulous enough, and the user isn't suspicious about, oh, this isn't a financial institution related kind of phishing attack, they might follow it. Whether it's viewing certain kinds of content, web albums, E-cards, you name it, the whole point of the fraudster is to get the user obviously to a page where they can infect either with a botted piece of malware or potentially crimeware.

The real take-away from this slide, and we all read about how looking just again within the spirit of what we call phishing has been evolving, the real take-away here is not so much the technologies and the methodologies and the approaches, I think what we're really seeing from our anti-fraud command center perspective is the prevalence by which these technologies and methodologies are taking place in uptaking.

When you look at, for instance, phishing-based,

man-in-the-middle attacks, they were kind of rare some time ago. It's common practice. You know, even over the last six to nine months when you looked at the price of phishing-based, man-in-the-middle kits, selling curled spam pages, it went from several hundreds of dollars or thousands of dollars down to a hundred or less, and we're really seeing a lot of price compression, certainly, in terms of the kinds or tools available, and we'll touch on that again in just a second.

A couple of take-aways here, not only from a growth perspective, we all see it. We all see crimeware growing rapidly, but clearly is the notion of how do we from an end-to-end perspective as and industry collected best protect. I think many of us who are involved with the anti-phishing group, there has been some terrific work going on there from either a registrar or registree's best practice.

Number one, just making everybody aware of how big and nefarious and problematic this issue is, but what are some of the very simple steps that we can do to expedite, once you identify sites or domains that are hosting whether it's phishing attacks, whether it's crimeware or what, how can we really expedite that time to shut down, blocking and shut down, obviously, and do

that, because when we think about signature-based desktop protection not being enough, and with the arms race ever continuing and with thousands of new variants always out there in the race to write a new signature.

In one example, our Trojan lab we looked at, we've heard of Gozy, or bank snippet, as it's also known as, in a single month it affected 30,000 users and before it was detected by AV. Just one variant out of the whole lot of them. It gives us obviously an idea of how big and problematic this issue is.

So, in terms of the price compression, or actually, I'm sorry, I jumped a slide there. Another point, and again this is a slide I've used in a couple of forums, is back to the consumer confidence and that impact on the relationship with whatever entity it is that they were working with, whether it's a financial institution or what.

This study, remember, this data point was from about six months ago, so it's a little bit long in the tooth, but the take-away is more than half of users, online users worldwide were already increasingly concerned about Trojans or crimeware, and while in our circles, we obviously know about this and we've known it intimately for some time.

Phishing, yeah, we can understand. We can

understand users being more and more educated and aware of phishing, but it's a rather telling statement when nearly half of online users, particularly in some areas that haven't yet been hit a lot by crime, the U.S. being one, relative to Brazil and Germany and other regions like that, or countries like that, it's a rather telling take-away. Certainly we expect this to uptake very rapidly.

Here's just one of a whole lot of examples that we could use, in terms of price compression. This is a fairly substantive and fairly capable Trojan and we've got to love the moniker super Trojan, as this fraudster who is a trusted reviewed vendor on one of the forums, had referred to it as. But you can see, and again, it's an eye chart, but for those who can't see it, just $600 for this piece of a rather sophisticated piece of crimeware. Compressing everything, all the tools in the economy coming down at I think a rather alarming rate.

Here's just one of many, many examples that we see as well, unfortunately we don't have a flash working behind this, but this is one example of some flash demoing or I should say flash advertisements that are being used in the underground. They are trying to get attention. They are trying to raise their hand and say buy my wares, buy my materials, and from a service

support perspective, not only have we seen a lot of crimeware, obviously there are a lot of these these days, but the vendors of these are offering patches or updates that if the latest AVA detects it, they're going to sell for $3.95, $5.95 a patch to what you have purchased. To basically say, okay, now this will bypass the latest AVA and your crimeware that you bought from me will continue to be meaningful and be accretive in actually lowering the ROI that you were hoping.

This is one example, and again, unfortunately, we weren't going to be able to show a video for the webinar purposes, so I'm going to go through a few screenshots. To qualify it, this is a very, very, very basic piece of crimeware. I had mentioned briefly before, there are two general classes that we are focused on, one is the identity theft crimeware, which will infect your machine through a number of ways, whether it was social engineering related, you think of all the social networking sites out there these days, Web 2.0, drawing people to possibly hit content or interact with content that will silently infect their machines.

The majority, still, will steal credentials when you, the infected user, go to a targeted site. It could be ten financial institutions and a few e-commerce

sites, for example, or hundreds of financial institutions, that identity theft, whether it's the key log-in screensaver or the local harming Trojan, will wake up when that user hits that target site, and then silently steal the credentials.

The other more nefarious, which we have obviously seen in places like Germany which is really driven by one-time password and strong authentication are those session hijacking or funds transfer pieces of crimeware that are going to be either in the background or take over that session once the user has logged off. This is a very, very basic version, and really it's just to demonstrate for maybe a few of you who haven't seen it in action before, how it operates.

Here's one called Limbo, version 1.5, gets back to our service statement, 1.6 is coming out next week and be ready for it, it's only going to cost you $2.95 as an example. It plays itself off to be a browser helper object, and so if we go to the genuine log-in page of our friends at Barkley's, this is how the page looks, and down below you can see the log file for the Limbo, basically the log manager call it for in terms of what credentials are being stolen, et cetera, et cetera. Here is the genuine page, and you can go through, you would enter your surname, membership number, just as a

genuine user would. So, that would be the real experience, and the machine is still clean.

What we do, then, is if this has actually infected a machine, the user would experience something different, and as I mentioned, this is a very, very basic piece of crimeware. This is injecting new credential-stealing fields. Name the field, and depending on the target, depending on the cash-out mechanism or vulnerability or whatever the fraudster is aiming at, they would obviously change the injected questions.

In this case, it's as basic or as simple as ATM number, ATM PIN. That obviously wasn't there before. Now, grant it, it's not perfect and there's still going to be a percentage of users who go, oh, someone is phishing, and I don't mean that in the pun sense, but something is not right here, but stepping up the game, certainly a more credible from a fraudster perspective approach than simply sending out phishing emails and relying on people actually responding in that sense.

So, what happens is the user would go through and if they fall for this, they would do the usual surname membership number, and oh, maybe this is some increased violation, maybe I have to put my numbers in here, my ATM number and pin, and they do that and you

can see you down below in the log the fact that it's actually being captured there and readily available or accessible by the fraudster to either use his or herself, or as we've discussed time and time again, sell it in the underground for a specified amount per credential.

You see here your Trojan configuration file contains special actions for different targets. That's a key point, you're always pushing out new variants. Do you want to do something different for a certain institution, aside from just trying to bypass AV, they might have different actions. They want to do per institution, and you can see some of those that have been censored here, but that's there in the code that you can see that goes into more detail about the Barkley-specific modification as well.

So, that's just one of the many, many, many, many examples that I know, actually many of us could probably share in this forum as well, to give an idea of the spectrum of tools that fraudsters are very, very commonly and frequently utilizing and employing.

One other, and I'm going to take just a quick tangent here. There's a whole scale or I should say assemblage of slides that I would often go into from a fraudster economy, latest trends, where is a lot of the

fraudster chatter focused on. You know, this is one that we're seeing in the U.S. While wire transfer has been and still is the prevailing cash-out mechanism for fraudsters, there's been a huge increase, and we've certainly seen a lot of chatter about fraudsters looking for certainly vulnerabilities and easily setting up bill payees. Either getting access to an account that already has billpay set up or getting an account and setting up a fake billpay address. Then that is one of the many mechanisms they might use to actually cash out.

So, a little tangent, but just kind of connecting the rubber to the road here a bit.

In terms, though, of what we should do, there are obviously many things. There are a lot of things that, whether it's financial institutions or other entities can do, but I think the real value here certainly, and going back to the comment before about what the collective, just for instance one entity, the Anti-phishing Working Group has been doing is raising the awareness of how big, how nefarious and how fast the threats are evolving, and from that baseline across all the entities and players involved in this system that we have here and all of us here is obviously then being able to put some very basic processes, levels of understanding, ways to engage in terms of saying, okay,

we have a site that's being hosted by this party here, this is the best way ultimately for us to get, say, that infection point shut down.

Again, we could wax poetic and/or prosaic for a while on best practices, but that's the quick overview. So, thank you for the time today, apologies for the throat, and I am going to pass it now on to Greg. Thanks a lot.

(Applause.)

MR. CRABB: Good afternoon. Thank you for giving me an opportunity to speak about a problem that I'm very passionate about, and I think that in the law enforcement community, it's kind of hard to understand all this stuff about malware and computer viruses and I think we as law enforcement officers have challenges trying to contend with these challenges, the complexities of these crimes, they're not user friendly. Most of our law enforcement officers, my law enforcement officer colleagues don't necessarily get cybercrime, but I think it's an important problem, because it goes to the heart of our business.

We've talked, heard about every panelist talk about the business impacts of these crimes, and I come representing an organization that is a provider to all of you, and that's the U.S. Postal Service, and as a

proud Postal employees, I hope that the work that we're doing in the cybercrime arena can help to improve the economics of the Internet, and that kind of gives you a perspective on why I come from a law enforcement perspective into supporting this arena, because it's about the business.

We need to be able to support the business users that rely upon our mail delivery services, our package delivery services, because these criminals are stealing the identity information of our consumers, and using those against our business infrastructures.

To talk about the malware economy, I came at this from a very odd perspective. I came at this looking at it from a financial crime perspective. This to me was not about a computer crime, it's about stolen identity information. It's about financial crime. All of the sudden, you end up in the middle of a botnet work with tens of thousands, hundreds of thousands of U.S. consumers' date on a laptop that's recovered from Eastern Europe, and who are the people that are behind these crimes that are responsible for this? And, so, that's the focus of my presentation.

My experience comes from a joint investigative intelligence initiative that I've been running with my good colleagues that Tom, the X-man Grasso opened up

this morning, and Special Agent Man Keith Mularski will talk about the National Cyber Forensics and Training Alliance tomorrow afternoon, but we've been working together for a number of years around this problem, and I think that we need not only law enforcement assistance, but we also need private industry assistance, because these are highly technical investigations.

The base of our knowledge is the work around the forums and a couple of speakers have talked about the forums, and together with the FBI, we've successfully conducted operations against a number of these forums. At one time, we were monitoring over 3,000 criminals that were engaged in some of the forums that are listed here. Fortunately, most of these are defunct now, but you can be assured that we are currently engaged in a number of operations that relate to the active world of these cybercriminals and their forum activity.

My perspective on malware from an investigative perspective has been around phishing. I had the investigative experience and fortune to be out in San Francisco for a number of years and worked some early cybercrime cases that related to the phishing sub-culture that developed in some of these forum arenas, and it's just, as you know, exploded over the

last five years.

Interpol is very active in combatting phishing, we've got an operation that we call Operation Gold Phish that has the participation of over 20 countries, law enforcement, plus private industry participation to attack the criminals that are using the malware to be able to steal identity information, and Gold Phish is kind of a misnomer now, because it started off as a phishing focused operation, and as soon as you figure out that you need some spam in order to facilitate phishing, you're well into the malware economy. Through this operation, we've shared and worked with law enforcement on over 500 subjects around the world.

So, who are these subjects? Who are the criminals that are behind this activity? And I've pictured, put pictures up of some of these people that we've run across in our investigations. Some of them have strong connections with Russian organized crime. Others are of Middle East dissent. Others are kids here in the United States who are engaged in the criminality of this activity. There is a prevailing youth behind these photographs. You know, a lot of these kids are young. You know, anywhere from typically 18 to 25 years old. However, that doesn't mean that organized crime in Eastern Europe or elsewhere have not gone to these

individuals and leveraged the capabilities that they've been able to develop to attack the computers of our consumers to be able to further their crimes.

So, I've got a couple of examples of forums postings that relate to the sale of malware. This is a posting that's on a Russian forum that we've been watching that the seller of this, his screen identity is Barracuda, and Barracuda sells a computer virus I think for about $300 U.S., and he will gladly take your money in a transfer on a digital currency called web money. This particular virus will do everything from steal identity information on the computer that it's loaded onto, or facilitate spam, you name it, it will do it.

And not only do these criminals conduct these activities for spam, it's also denial of service attacks. This particular bot was used in the highly publicized Estonian D-DOS attacks. Here's his Avitar logo, and some of the controlling channels, screenshots that some of the controlling mechanisms behind his particular bot.

And then a target that has been a thorn in my side for a long time, but is definitely something that needs to be recognized as a problem, and that is these criminals are outside the United States, not only was the writer of Barracuda outside the United States, but

this individual, Smash, who he's been written up in the press quite a bit, remote access Trojans, RAT systems, was the website that he sold his particular virus from, he is definitely not in the United States, from Eastern Europe, and we have trouble as law enforcement officers being able to bridge the gap between these crimes and something that's recognizable on the books of foreign law enforcement.

In monitoring the cash flow, we do a lot of different types of investigations against these subjects. We'll trace the communications, we'll trace their money flow, we will try to do whatever we can in order to get back to the true identity of the individual, and in this particular instance, we were able to trace some of the proceeds, and some of the communications of this particular individual with some subjects in the United Kingdom, and for me it wasn't a financial crime investigation.

The subject was using this particular virus that was sold by Smash to steal identity information, identity information of UK citizens, and it looked, smelt and felt like financial fraud to me, and in November of 2004, I had an opportunity to write a report to the UK on a subject that was using this virus to steal identity information.

We provided the report to him, the subject we monitored some of his communications, he was a Muslim living in the UK, and this particular chat that we recovered, the community thought that he was trusted because he was of Muslim dissent. Fair enough. But when it came down to it, he was later arrested by New Scotland Yard, their National Terrorism Financial Intelligence Unit, for conspiracy to murder, incitement to commit terrorist acts and possession of articles for terrorism purposes.

Now, obviously the financial crime that was related to that is maybe not as significant, and but these criminals not only have financial intent, but we're starting to see more and more where the subjects are based in the Middle East, and have terrorism as a motive.

There was a nice write-up in the Washington Post a couple of days ago, about this particular case, and its tie of how spam and email was associated to stealing identity information that was used to be able to fund this activity.

So, I hate to leave or end on this particular note, because the mass majority of the crime that relates to the malware economy relates to financial crimes, but we have to be cognizant of the fact that we

are on the verge, I think, of seeing more and more of these terrorism organizations and others trying to penetrate our networks, to further their schemes. Fortunately in this case, all three of these individuals pled guilty, I think it was July 4th, and were sentenced on July 5th to sentences between I think seven and ten years, but we need to take these crimes seriously.

And on that note, I want to turn it over to my colleague, Heinan, and thank you very much.

(Applause.)

MR. LANDA: Hi. Oh, good, I love it. My name is Heinan Landa, and let me give you some context. I'm going to actually be flipping a coin a little bit, looking at the other side. We've seen a lot about how spammers and those perpetrating malware can actually make money. Now let's look at the side from the point of view of small businesses. And small, medium-sized businesses in the United States and what kind of damage, financial damage, and other types of damage, that these types of malicious software can cause.

Let me give you a little context. My company is Optimal Networks, we're located right up here in Gaithersburg, and we are providing IT outsourcing and network support services to small and medium-sized businesses, exclusively in the D.C. area. So, my

clients might range from a small size of about ten employees all the way up to about 200.

And when I first accepted the honor of being on this panel, I was thinking, oh, this will be fun, I'll come out and talk a little bit about spam, we do quite a lot with spam. In fact, we are now offering what are called managed services, which is a fixed price per month per PC where we basically promise our clients to do all the preventative measures against all the malware, spyware, anti-virus, anti-spam, patching, all that kind of stuff, so the cost of this prevention and the cost of recovery is actually very important, because it affects our day-to-day business operations.

So, I said, this will be great, I'll come and talk about our clients, the effects of spam and the effects of spam prevention on our clients. But when I was starting to do research, and I'm not sure if you're aware, but as far as an economic force, small businesses in the United States comprise about 50 percent of our nation's GDP, non-farm. So, it's 50 percent of the gross domestic product, which is six and a half trillion dollars.

That's a major, major economic force we're dealing with. So now I feel like I have to actually stand up straight and wear a tie and talk about it.

So, let me start with a few anecdotes. So, you can understand qualitatively what malware can do to these small businesses, and I actually solicited some input from all of our clients to see if I could give you some actual hands-on stories, and one of the first places where our clients were affected very dramatically by spam, and you saw this in the previous panel, was in the directory harvest attack.

So, this is when the spammers are trying to acquire the addresses to spam to. They are bombarding email servers with false emails. Right, trying to figure out which emails, addresses are correct for those servers.

Now, let's take a look at this, away from the consumers. Most consumers are using the email servers in their Internet service providers, Verizon, Comcast, they're using those email servers. Most large businesses have their very robust email servers. Most small businesses also have their own email servers, but they are not quite as powerful as what you might see in the large businesses and the Internet service providers.

So, when a spammer tries to harvest addresses from one of my clients, and I'm talking particularly about one of my first clients who got hit with this, a

30-person trade association, and they started pummeling that server with tens of thousands of email messages every day, and opening up direct connections into the server, trying to find out the addresses, and that server said, oh, I don't know any of these people, and started trying to bounce back, hey, this is not deliverable, this is not deliverable, this is not deliverable, and then they couldn't get it through those messages, had to wait four hours and do it again and again and again. It was a matter of two days before the server collapsed, just knuckled under.

This started happening client after client after client, because I don't know if you're been following, but there's really been an explosion of directory harvest attacks and it's increasing dramatically, and you can see why.

The only solution was for them to incur yet another cost and put in more spam filtering software on the network and engage in outside spam filter, which put them out of commission for a week. On average. Across our client base. So, that's one aspect of it.

Another aspect of it is a church. One of our clients, when we first got to them, one of their senior pastors had received a spam, clicked on it, malware infected their system, lost years and years worth of

documents, spreadsheets, Word documents, just wiped out his system right there.

My client writes me that it cost him thousands of dollars to recover from that, and to this day, four years later, they're still not out of the effects. They needed that information, they were storing that information for their parishioners and they were using it to run their church. So, how do you measure that? I'm not quite sure.

One of our clients is about a 70-person company in Rockville that manufactures specialized baby food. They are using the spam filtering service, they have about 25 salespeople spread across the United States, and their IT director estimates that even with the spam filtering, the multiple levels of spam filtering that they have, they have still lost ten full days of productive salesperson time because of malware, caused by spam.

He also says where he used to work, it was a 200-person organization, $50 million a year, and some worm got in, via email, and attached itself to their anti-virus program, incapacitated the entire company for three days to an estimated cost of $160,000.

So, I'm just trying to give you a sense of the magnitude of what's going on here. If we look at it

financially, there's two main areas where I see the financial damage that malware is causing. The first is once the spam gets through, the malicious spam gets through, and does something, it wreaks havoc in one way or another. There's a cost to recover from that.

The second are all the measures that we have to take on an ongoing regular basis to prevent this from happening. So, let me talk about the first first. Because that's good engineering. One, two, three.

The damages. What kind of damages can we have? We can have lost data. Right? Very common. This is like what happened to the church. So, the malicious ware can come in, it can wipe out your documents, it can compromise your accounting data, it can wipe out your customer lists, it can do all sorts of damage to data, specifically.

So, the cost can be measured in several ways. The first is, what does it cost to restore or recreate that date? Right, now this may be an hour of a consultant's team, and you should know most small businesses do rely on outside consultants, so it is more expensive than having your own internal person.

It could be an hour of a consultant's time to restore from back-up, or it could be hiring an army of temps to retype in data. So you really don't know. It

depends on the specific situation, but that's one cost.

Another cost is you have a bunch of employees and they're sitting there twiddling their thumbs while the data is being restored, right? They may not be able to use their system, they may work on secondary tasks or low priority tasks or in some cases they get sent home. So, what is the cost of that lost productivity?

Then there's the issue of lost opportunities. If a client calls in and wants to open up an account, or wants to do a transaction and you can't because you don't have their data right in front of you, that's a lost opportunity. This could be immeasurable, but it's very large.

Finally, you have what I'll call the soft costs, the reputation. What is the harm of your reputation if your clients calls you and you can't pull up that last invoice that they're talking about, because you don't have it. All right, what is the cost to your reputation? And then what is the cost to your internal morale? I don't know if any of you have ever experienced this, when you get a new computer, your morale goes up, it's fun. Hey, my company cares about me, my agency cares about me, I got a new computer, I'm really happy. The opposite is true when you can't use it. It's frustrating, you feel powerless, and morale

goes down.

So what is the cost of that to a business? Especially a small business whose employees are really what make it run. So, that's one aspect of the damage, lost data.

Second might be, or is, how should I put it, a crashed system or the inability to actually use your systems. Now, in some cases, with the directory harvest attacks, or also there was a situation where a bot got inside of a network and was broadcasting spam out, effectively denying that company its use of its Internet access, so email servers go down, you can't use email, you can't use your machines, your server has crashed, this is basically inability to use your system.

So, you have costs again. Your costs to recover. Your costs to restore your system to an operating state, right? Are you reformatting your server? Are you buying a new one? In some cases, you look at it and you say, oh, my God, this server is three years old, and it is going to be more cost effective to buy a new one, install it, set it up and run it than it is to try to recover from this disaster that just got hit by malware.

Whatever it takes to restore it to an operating state. These clients that I recommended they go on a

spam filtering service, like Postini or MailWise, in order to prevent from that, they had to do it, and that wasn't a one-time cost, that's an ongoing monthly cost that they need to spend to make sure it doesn't happen again.

You have opportunity costs. Yesterday, I had a conversation with the president of one of my clients, they're a real estate firm, and they're involved, they're local, they own quite a bit of land, they're very small, about ten people. They are involved in a huge, huge deal in California. It's all secret, it's all hush-hush. This guy said his email is now so critical because this deal is going to close in two weeks and he's watching this minute by minute to make sure and to let him guide it in case it starts going south, he can pick it back up. You know? If he loses that, the ability to use his email, if his server goes down, due to malware, if it chokes up his Internet connection and he can't get his email, he could be looking at multiple millions of dollars down the tubes. Huge. That's lost opportunity.

Again, there's the soft side of reputation. I hate to see mea culpa, but a little while ago, we were putting out a new website, and it got infected with a bot, where every time you go to the site, it tries to

download on your Internet Explorer something to ravage your mornings or I don't know, luckily I didn't want to know what it was going to do.

Now, what kind of reputation is that for an IT company to have a website where people go to it, and there's a bot there? You know, it's horrible. I mean, luckily we were able to recover inside of 30 minutes or an hour, but that can go on a wider scale, and it's something that you can't quantify. Again, it goes to morale. What do you think my staff, my employees thought when our website had that, but even more so, when people can't use their systems. Because they need to work.

Finally, the last area of recovery is in terms of compromised data. All right, whether it's through phishing, whether it's through key loggers, whatever it is, it has a few areas where cost come up on that, the first is the loss of competitive advantage, loss of some sort of information that's critical to your business that you don't want your competition to get. That's a major area of cost. Dollars stolen. Issues, again, like reputation.

We had a client who this actually wasn't malware, somebody broke into their office and stole their server and walked out with it, but the effect is

the same, they lost 5,000 credit card numbers that they had to take and fax each and every one of their customers and say, we lost your credit card number, you might want to change that credit card. What does that do to your reputation?

So, because these potential damages are huge, they're monstrous, companies, small businesses, large, everyone is doing whatever they can, and are spending significant money to mitigate these risks, and that's where we get into the preventive measures, okay? You've got firewalls, you've got like physical hardware that you can put on your system, Andy from SonicWALL, can I say, can I say? SonicWALL. There's your plug.

MR. KLEIN: I'll give you a dollar.

MR. LANDA: Thank you. Firewalls, VPNs, encryption, SSL subscriptions, all of those networks in place to increase security, prevent this type of malicious ware. Anti-virus programs, on each and every computer, on servers, on your email, on laptops. Anti-spyware program, same thing across the board. Spam filters, on the network, off the network, many, many different solutions, many, many different companies putting them out.

Patch management, all of the operating systems and the software, Microsoft Office, Internet Explorer,

so on and so forth, are vulnerable, and become more vulnerable, and need to be patched. So, how do you make sure, now that you're patched. You know on your computer you can go and click on the little button and do Microsoft Update. How do I as a business owner make sure that every computer in my company, whether it's on the network or off the network, is going to be patched? That takes software, it takes hardware.

User education, which ranges from the Draconian, if you're not expecting an email from someone, delete it. All the way to classes on how to detect phishing and so on and so forth. There are significant costs in user education. The cost of professional IT management. Consultants, managed service plans, whatever it is that these small businesses often don't have in-house and do need to contract outside. So, the cost of prevention is rather high. The cost of the professional management, the outside consulting and support and the user education is often as high or higher than the actual outlay for hardware and software. To execute the security measures.

So, let me leave you with a few thoughts. Small businesses represent 50 percent of our nation's GDP. Over six and a half trillion dollars a year. While they are the most powerful group in aggregate, the most

powerful economic force, when you break them down, each one of them is actually the poorest, because they're small. They don't have the resources, the financial resources that these large companies have to prevent against this, and it's not as economical for them to do so. They don't have the internal IT management infrastructure to do this, so they have to turn to outside consultants and outside services like my company and thousands of other companies are providing across the nation. So, they have to spend a disproportionately large, a disproportionate amount of money for the preventative and recovery efforts.

With the advent of managed network services, that I kind of briefly touched on where it's a fixed price per month, per computer, that helps, that helps contain the cost, but this is some very new stuff and very, very few small businesses are on these kinds of services yet, and it's still a lot more expensive, proportionately.

So, I guess my plea here is that anything that can be done to help mitigate the cost and the complexity of fighting malware, especially if it's geared toward the small and mid-sized businesses. Not only will we have a significant negative impact on the malware economy, but I think it will have a very significant

positive impact on our nation's economy. Thanks. Thank you very much.

(Applause.)

MS. DREXLER: Thanks so much, Heinan, and all of the other panelists. I am going to ask one quick question before we move into a short period for audience questions and answers. I'm hearing that some of the incentives for these cybercriminals are the low cost and you can attack thousands of people at once and that the cybercriminals don't need to re-invent the wheel because they're trading this information back and forth in all these forums and then launch these anonymous remote attacks and what this results in is there's damaged business reputations and lost data and many other costs and we could go on and on.

So, what I would like to know is who exactly are these cybercriminals? We've heard everything that they're kids in their basements to these organized groups online, whether it's organized crime that's moving online, or whether it organized crime that's being set up as a result of that. I'm wondering who they are and whether your public forums contribute to that and where are they all going? Would someone take a moment, whoever wants to start?

MR. KLEIN: Sure, I'll start. I think it is a

combination. The interesting part about it is there doesn't need to be, like I said earlier, a building where they all go. As a matter of fact, that probably makes no sense at all, but the Internet infrastructure, the communication infrastructures that are out there that allow people to congregate and talk in chat rooms and such are where they come in, and what their age is, age is only because they're youthful because they've been brought up in that environment and they're not afraid of it. Many of us were around before computers really took off, and so not that we're afraid of it, but we just weren't brought up in that environment.

So, I think you see youth, but you see youth because they're the ones getting caught. I think there's a fair number of professional organizations in some of the foreign countries, over in Europe and such that utilize these resources, these youngsters to do the types of things that are necessary, pick up those pieces and develop the pieces and then organize them and take a small cut out of that whole process, but I don't think, like I said, there's no malware building where you can just go and arrest a bunch of people, because there doesn't need to be, it's just a cyber community and nothing more.

MS. DREXLER: Anyone else?

MR. HINRICHSEN: I'll take a slice of not so much the who or the what, but the how. You know, you think about many of the exchanges or the communication or dealings between fraudsters and the underground and you can bring him on separate forums, they had even created their own communication channel called Carter IM as an example, some time ago, but a recent instance in an actual automated online store for credit cards.

So, when you think about being able to expedite a particular fraudster, whomever, wherever they are, whether they're part of an organized ring, whether they're an independent individual of any age, it just shows you how easy it is now for the passage of goods and the commerce of goods to occur.

So, instead of having to go off into an ICQ channel, barter with that individual, get to a certain price, it's a store. Just like any other e-commerce store that's available in the U.S. and Russian language. You know, you pay with web money. So, the process itself continues to evolve, very much like our very public e-commerce as well.

MS. DREXLER: Great, anyone else?

MR. CRABB: Great, and I'll add on to that, having had an opportunity to chase a number of these communities around the world. I refer to it as

networked criminality, in that the organized crime cells or the individuals can hook into the network, get what they need out and do with the information that they've stolen or the services that they've provided into the network as they may.

I don't really care what you've done with the information, I just want my money out of the operation perspective. It's organized crime in Eastern Europe, we've seen Ukrainians, Lithuanians, Russians, organized crime all connecting into the network.

I've had the opportunity to go to Nigeria on a number of occasions that relates to this type of activity, where in an economy that is so desperate that it doesn't cost a lot for large groups of people to be able to connect into the infrastructure, get out of it what they need, and go on, so all they need is a cyber cafe. They're hooked into the network, and they can amass the lists that are necessary to spam and be off and running in a very good phishing operation in a very short order.

You know, you also see the Eastern Europeans, or not the Eastern Europeans, the Middle-Eastern nationals engaging in this as well. I've had the opportunity to do law enforcement actions in Egypt and Jordon and Lebanon. We see more and more of these criminals, just

wherever they may be in the world. The modus operandi is all connected into the malware economy, and we are going to see more and more of it.

MS. DREXLER: Great, thanks. I assume, Heinan, you don't have anything to add. We will take some questions from the audience now. If there are any. One of the questions is, are there any estimates of how much revenue per year the spammers make and what the total costs are to the U.S. economy?

(No response.)

MR. LANDA: I don't have any of those.

MS. DREXLER: I think during one of our breaks, we may have had actually a question regarding this, just generally about cybercrime, I don't necessarily know that it's more geared towards spammers, but I don't know that we have the breakdown right now, but maybe we could try and find out that.

MR. LANDA: It's very tough to break down the costs, because you have, for example, the stuff that I talked about. When you look at each one of those individually, it's so situation-specific, and some of those costs, especially when you are looking at opportunity costs, lost reputation, loss of morale, which can lead to turnover costs, and they're very, very hard to pin down. I can tell you that internal service

delivery costs, people estimate, are between, for IT service, are between three and 15 percent of the revenue of the company, but I would hate to take that and try to draw a dotted line to six and a half trillion dollars.

MS. DREXLER: Okay. We have a question specifically for Jens at RSA regarding the Barkley browser helper example. Would this attack be as effective if the script were available in the browser or limited in tools like the Firefox no script extension.

MR. HINRICHSEN: One more time.

MS. DREXLER: It says for the Barkley browser helper example that you gave, they would like to know would this attack be ineffective if scripting were disabled in the browser or it was limited with tools like the Firefox research extension?

MR. HINRICHSEN: I can't speak to the specific variants, but certainly there are ways that it becomes ineffective or is otherwise disabled. You know, if I were in our CTO's office, I would wax more prophetic on that.

MS. DREXLER: Thank you. Are there any other questions from the audience?

(No response.)

MS. DREXLER: Okay. Another question I had is if we could look at a little bit more into the role of

fear and trust, and how social engineering plays a part in allowing this to happen and as one of the incentives for these cybercriminals. Exactly what would you say are the biggest factors in allowing these attacks to happen that motivates these cybercriminals? Anyone can respond.

MR. KLEIN: Well, I would say about three years or so that we've been running something called the phishing IQ test, which is a fairly straightforward mechanism for people to go in and see if they can identify phishing or legitimate emails. It's consumer focused, it works pretty good. But over the length of that time, we've seen the way people perceive these messages change.

Initially, when people were taking tests, there wasn't much out there in the way of phishing, for example, but they were actually, weren't very good at detecting phishing emails. Which made perfectly good sense. It was kind of unknown to them, they didn't know, and they were very good at picking out legitimate ones. Over the three years or so, that's flip-flopped completely, so that now they're fairly good, about 90 percent, at picking out phishing emails, but legit hate ones, about 50/50. It all goes to the notion of trading trust versus protection. That's kind of the general

conclusion we've come to when you talk to folks about it, and you see it in the data that's out there.

So, I think that's the trade that people make. We've heard earlier that people are going to continue to use email, and I think I certainly agree with that. But it's what they have to do on a day in and day out basis in order to utilize that is make that trade of protection versus trust.

MS. DREXLER: Anyone else?

(No response.)

MS. DREXLER: Any other questions? We have a question over here, if you can just wait for the microphone, please.

MR. FOX: Hi, Jeff Fox, Consumer Reports. Just wondering how easy it is for someone to find their way into this economy. There's so many people doing this and you've got all these kids and young people. I know they're tech savvy, but I mean, do you just find it by Googling the right term, do you have to wander around all the IRC chat rooms? You know, I'm not asking for specific details.

MS. DREXLER: Are you looking for a new job?

MR. FOX: Is it that easy to find, because so many people obviously have found it. Do you have to be friends like with a bunch of criminals?

MR. LANDA: I think it's fairly simple. I could give you an example, I might not want to share, but my daughter hacked into my iTunes account, so you think, oh, my God, how could this happen, this is an IT man, doesn't he secure his systems. So she went and she hacked into my iTunes account in order to give herself money in her iTunes account so she could buy a few more songs. So, it was more or less innocent, but we --

MR. CRABB: We call that friendly fraud.

MR. LANDA: Friendly fraud. How did she do it? She went into my iTunes account, said she forgot the password, clicked on the forgot password button and just started answering the questions. What's your mother's maiden name. She knows. She didn't know my birthday, so one day at the office I got a call, daddy, what's your birthday, and I'm thinking, cool, she's buying me gifts. But it's not that hard. She's --

MS. FOX: Social engineering.

MR. LANDA: She's 11, she's very, very deep into all of that cyber world, and she's a good kid. I don't think it would be that difficult for someone to really get involved in the negative aspect of it.

MR. CRABB: And just to comment, the forums are very easy to find on the Internet. The forums are easy to find, criminal organizations are talking about

cybercrime. You know, the statistics show that cybercrime is as lucrative as the drug economy is today. So, why not go to cybercrime? The criminals will talk. They direct themselves into those areas.

MS. DREXLER: The second part of Jeff's question, how easy is it? I mean, do you have to be into the organization? They're obviously very easy to find and go to them, but are you able to actually purchase these without knowing somebody?

MR. CRABB: It's very easy. It's the development of untrusted relationships and the underground economy. The anonymity of the types of transactions, the financial transactions that they make between each other, the criminals do not know each other. They're sitting in remote locations. I say that the criminals do not know each other, the disparate criminals do not know each other. Criminals that are operating and as organized crime cells that hook into this network obviously know each other, but it all depends on where you get stuck into the economy of the criminality.

MS. DREXLER: Do you have another question?

MR. LEIBA: Hi, I'm Barry Leiba. In relation to the last two questions, by putting these I-forgot-my-password questions, we're inviting problems

with this sort of thing. First of all, those sorts of questions, what's your favorite pet's names, what's your mother's maiden name, are ideal social engineering sorts of questions, and apart from that, we're basically asking people to pick insecure passwords to get their real passwords from. You know, I could guess that your mother's maiden name is more likely to be Johnson than some other stranger thing, and many times I might be right.

On the general thing, we're doing a lot of things, the legitimate sites are doing a lot of things wrong that are making people, I guess it was to Andy's comment that people are less sure about real sites now, because the real sites are making mistakes, that make them look less legitimate. They're hiding the SSL behind a Javascript button or something so that you don't see the little lock symbol because your conversation with the server isn't secure until you push the button, and then whatever you entered is transmitted through using SSL, but it's hidden from the browser interface.

We're doing a lot of things like that, self-signed certificates, expired certificates that are causing pop-ups to users, and they're starting to get used to seeing these things, and sometimes it means they

trust untrustworthy sites because they're answering yes to these untrusting pop-ups. The second thing is the sites look bad because of these pop-ups. I think we have to fix that. Legitimate sites have to be very careful to do the right things.

MS. DREXLER: Thank you.

MR. LEIBA: A bit long-winded, sorry.

MR. CALSON: Hughy Calson. There's one other cost that I don't think I've heard anyone mention yet. It occurs to me that the one reliability method that has been found to make spammers stop sending spam is to take away their computer and give them a room that has no door knob on their side.

Now, we've heard the FBI say they've had some success, we've heard the FTC say they've got a dozen cases, we've heard Jon Praed say that civil attorneys can handle a lot of the investigative work and push a lot of these cases much better than government can.

My question is, there's hundreds of them, there's dozens of you. Who's going to pay for ten more Jon Praed's, for ten more FTC staff attorneys and legal clerks? We're going to need some more FBI guys.

MS. DREXLER: I think that's a great question. We're actually tomorrow going to be having a panel on law enforcement issues, so hopefully we can address that

a little bit more in that. It looks like we have another question, and I think we have time for about one more question. So, go ahead, thank you.

MR. CROCKER: Dave Crocker. I was listening to Barry Leiba's comments about the various things that make it easy for users to make the wrong decision and I was trying to listen to that as if I didn't have any background in it, and I went kind of crazy, because there is no way it's reasonable to expect any normal person to be able to make the kind of distinctions we're forcing on them.

It isn't enough to say that a given site needs to follow some good practices, because what he was describing was an Internet-wide systems design problem. We have established patterns that no single site can fix, and it struck me, this is a category of problem that's exactly perfect for an organization like the FTC to look at. There are guidelines, guidance, conformance rules, I don't know why, that needs to make the life of the user vastly simpler for making assessments about trustworthiness of where they are and when they're clicking.

MS. DREXLER: Thank you. I think tomorrow we also, in our consumers panel, we will definitely be addressing some of those issues as well. I want to

thank all of our panelists for being here today, thank you all for listening, and we're now going to take a short break for about 15 minutes, and we'll convene again at 3:30. Thank you all very much.

(Applause.)

(Whereupon, there was a recess in the proceedings.)

EMERGING THREATS

MS. CHRISS: Okay, everyone, we're going to go ahead and get started here. So, feel free to take your seats, and welcome back. Please, congratulate yourselves, this is the final panel of the day, and you all have been a wonderful audience. So, thank you.

Has everyone settled in? All right, terrific. My name is Sana Chriss, and I am the spam coordinator here at the FTC. Admittedly when I first mentioned that to someone, they said, well, that doesn't sound very good. So, I had to clarify, I'm against it, I don't actually coordinate it, I am against it, and I work with many of my brilliant colleagues to develop strategies for fighting this ongoing spam problem.

So, this panel is called Emerging Threats, and what does that mean and why is it important? We're going to examine all of the things that you've heard about today in terms of how they are affecting other platforms, whether it's mobile devices, social networking websites, or voiceover Internet telephony. We're going to examine what are some of the future threats that are happening and how can we best protect consumers, because at the end of the day, that is what it's about, whether it's consumers or customers for you, we're all trying to achieve the same goal.

This panel is important because it gives us an opportunity to really be proactive, and I think I'm going to speak for the agency in saying that's something that we really do best. Our first spam-related case was in 1997, okay, and CAN-SPAM, the CAN-SPAM Act became effective in 2004. So, that's pretty proactive, if you ask me, using our authority under Section 5 to combat fraudulent and deceptive acts, regardless of the platform.

So, the industry members before you, they are similarly situated in that they are on guard in terms of being vigilant in protecting their customers from these emerging threats and they, too, are very proactive. So, let me introduce some of these wonderful panelists today.

Next to me is Mike Altschul, he is the senior vice president and general counsel of CTIA, The Wireless Association; Dave Champine, he's the senior director of product marketing at Cloudmark, which is a provider of carrier-grade message security; next to Dave is Scott Chasin. Scott is the chief technology officer for MXLogic, and MXLogic is a provider of managed email and web security services. Scott is also the chairperson on the MAAWG subcommittee fighting spam bots. So, he will have something interesting to add there as well.

Next to Scott we have Rick Lane. Hi, Rick. Rick is here, he's with News Corp., he's the vice president of government affairs, and as you all know, News Corp owns MySpace, the social networking website.

Next to Rick we have Christopher Rouland. Chris, he's a chief technology officer and IBM Distinguished Engineer working with IBM Internet security systems, which advises thousands of the world's business organizations and governments.

So, I think that you will all agree that we have some experts here on this panel, and so without further ado, Mike, would you like to get us started?

MR. ALTSCHUL: Are the slides controlled? Oh, you can control the slides. I don't have to stand upright. I will. Thank you.

Well, and thanks, again, to the Federal Trade Commission for inviting us to participate on this panel, and convening these two days.

I was fortunate enough to participate in the first of the spam forums, a little more than, what is it now, four years ago, May 2003. At that time, we recognized that wireless spam and malware was going to be an important thing to our industry, CTI represents wireless carriers and their suppliers and indirectly the 240 million Americans who are wireless customers.

We were a bit behind the rest of the world in rolling out text messaging and some of the data applications, and had observed overseas the explosion of spam, which really colored and spoiled the user experience. So, sometimes being second isn't such a bad idea.

We have the opportunity to learn from overseas, and we're able to deploy our first generation of these data services in a way that has been, I think, while not perfect, remarkably successful in protecting and filtering spam and malware from wireless users and device.

I'm going to be talking about where the industry is going, though, and as we move forward into basically converged Internet devices, where phones are increasingly web browsers, we will leave the protection of the walled garden and some of the filters and protections we've provided.

So, that's a little bit of background as to how we got started and what I'm going to be talking about. We now have, by our measurements, as I said, 240 million subscribers, and more than half of them have devices which can be used as Internet browsers of one kind or another, 56 percent of wireless devices in the U.S. can access the public Internet.

The first slide that we see before you just makes the point that anywhere you can go from your desktop, using a cable modem, DSL line, a satellite broadband over a power line, WiMAX, WiFi, whatever, increasingly you can use commercial wireless device to get to.

A little bit surprising, if you haven't used it yourself, but in the last year, 18 months, our industry has aggressively rolled out what are called 3G, third generation services that now offer true broadband speeds. Now there's a debate in broadband policy circles as to what is broadband speeds.

So, we haven't used that term so much as identifying equivalents to DSL, which is the typical telephone company offering, or cable modem services, but each of the national carriers, regardless of their technology, is now offering DSL-like speeds to their customers, particularly in the major markets and increasingly in the smaller markets across America.

Sprint has announced for later this year the deployment of the first fourth generation broadband wireless service, WiMAX is the name of the technology that's offering a theoretical maximum download speed of 20 megabits per second, which puts it in sort of cable modem territory.

We're going to have the opportunity in the Washington market and in Chicago to be the early adapters and to actually see how early adopters, not adapters, early adopters, to see how close they come to these speeds, because Washington and Chicago are going to be the first test markets, trial markets, so be turned on.

As this third slide shows, consumers increasingly are using wireless phones and device to access information and the form factor is changing accordingly, so that we are all familiar with the iPhone and I almost brought our office one today, but somebody else had checked it out. The screens and functions are less and less like a traditional telephone, and more and more like the screen on a laptop or PDA.

So, there's a couple of wonderful websites that you can go to and see all the different products that are available in the market in the U.S. We've counted more than 200 of these 3G broadband devices. They include something called air cards, it's basically a card that slides onto any port in a laptop and is basically a wireless broadband connection that will allow a laptop to do anything a wired connection to the Internet will provide.

This is just a partial list of the number of

hand sets with web browsers. You may recognize some of the names, and similarly, another way of accessing the Internet using wireless devices is with WiFi, there's WiFi in this room, if you have a WiFi enabled smart phone, you can get to the Internet, either using the carrier's commercial spectrum or using WiFi from any WiFi hot spot.

The industry has the benefit of the CAN-SPAM Act that I think you're all familiar with. In particular, the FCC implemented CAN-SPAM with particular rules for commercial mobile services so as to prohibit the sending of any unsolicited commercial messages to wireless devices, and the FCC has created a website and registry much like the Do Not Call Registry where wireless carriers are obligated to list or provide lists of the domain names that they have in use for wireless device, and spammers, at least law-abiding spammers, are obligated to go to that website, download the list and not send messages. Carriers have been aggressive in going after and suing those spammers who they can find in the U.S. and who have not been diligent about this, as heard on the earlier panel, and you all know most of the spam seems to come from outside the U.S.

But we do have legal protections which are unique to wireless device. You probably all know that

there are at least two types of wireless messages. One, I'm going to hold up my own personal BlackBerry as an example here, one is something called SMS, or short message service, and MMS messages. These are primarily peer-to-peer text messages sent from one mobile device to another. Then the other are email addresses which are sent just as an email message is sent from any computer to any other email address.

The distinguishing feature for an SMS message is it uses a telephone number, a North American ten-digit telephone number as the address, and is limited to 160 characters as a message cell. An email uses the traditional Internet domain address with the @ sign and a high-level domain name. This one BlackBerry has five different addresses. I can get the identical message sent to this device and then I can send the identical message from this device five different ways. First I can receive and send SMS messages just to my phone number. For those lawyers in the room, SMS messages probably are not covered by CAN-SPAM, but they're covered by the Communications Act, because they use a phone number as an address.

I also can use a PIN, BlackBerry has its own server, and all of the BlackBerry devices have a serial number, basically a PIN, and if you know, and we know

within our office the PINs of all the users, you can use that PIN as an address, the message will never go to the public switched network or the public Internet, it will just go to the BlackBerry service and then back down to another BlackBerry device.

As it turns out, during September 11th, PIN to PIN BlackBerry messages were probably the most reliable, least delayed ways of communicating because it really didn't touch the public Internet. Also, at that time, there were a lot fewer BlackBerry users than there are today.

I also can get, receive a message sent over the Internet using the AT&T Gateway to this device, if you use my wireless number @ATT.net. That is something subject to CAN-SPAM, it's a traditional email message that is sent over the public Internet. It goes through a Gateway that AT&T provides for its users.

There is spam filtering and malware filtering at that Gateway and it's delivered to this device. Because it's a BlackBerry, it also mirrors my desktop at work, so my office email address, all those messages show up on my BlackBerry device, and I can respond and send messages using my office email address. I have downloaded a Google application which also synchronizes by personal Gmail account to this device. So, just as I

can get all the email sent to me at my work address, all of the personal email sent to my Gmail account also comes. If you count those, there are five different addresses with at least two sets of legal rules, and five different ways of introducing spam and malware into this device.

So, those are some of the challenges that we're all facing. While it's possible to send spam messages through the carrier's gateways, one or two messages at a time, carrier's gateways have been effective in identifying and filtering out real spam attacks. So, a one or two may slip by. First, that may be cumbersome to send multiple messages to a large list or certainly to all the users using phone numbers, and they're very effective in identifying spam-like messages.

When you start moving into email, and email that comes to devices like this from outside of carrier gateways, my protection from spam on my office email is only as good as our office IT department's protection. My protection from spam on my Gmail account is only as good as what Google and Gmail provide, or what I may provide for myself.

I'm not going to get into the debate about net neutrality and the proliferation of device. I know someone from Consumer Union is here, Consumer Reports,

every February reports on wireless device, and I hate the fact that there are so many different operating systems, so many different technologies, we have GSM, CDMA, CBNOS, Microsoft NOS and so on.

In an ironic way, that has been very good protection from users of malware, because there are so many different standards and technologies being used, and no one truly dominant operating system or technology, the diversity and robustness that we have as an industry, I think, has been a benefit. Just as sort of the Apple Microsoft operating systems have been more of a benefit to the Apple model.

Similarly, as we move from closed systems and walled garden kind of applications, to more open access to the Internet, more open access to side loading and downloading content and applications on these devices, carriers' ability to protect and vouch for the security of the network and the applications is going to diminish.

This is just natural, the same thing happened when the users demanded more openness than the original Prodigy model, or even the original AOL walled garden model provided.

So, we started in an environment where carriers operated under pretty much of a closed walled garden

environment. As users have gotten more and more experience with the Internet and with wireless devices, they're demanding more openness, more applications, and with that, users are going to have to start taking more responsibility just as we do with our own desktop situations, for protecting themselves against malware and spam, and we will not be able to rely as heavily on carriers and networks to do it for them, because carriers and networks are going to have much less control over the user experience. It's not good or bad or trade-off, it's just what's going to happen as the industry responds to the public's desire for more open access.

So, I think that's pretty much it. I just, I also want to close with this final slide, which at least to me I find amazing. This is a graph taken from the FCC's most recent report on high-speed Internet access services. They're so-called broadband report. They measured the last six months or the time frame from basically January 1 to June a year ago 2006, and in that time, which is just coinciding with the rollout of 3G networks by the national wireless carriers, 60 percent, 59 percent of all new broadband services or customers were wireless. Not our own growth, from a low base, but we added more subscribers, subscriber lines, whatever

you want to call it, than DSL and cable combined. We're quite confident when this year's report comes out, we're going to see continued extraordinary growth and acceptance of these wireless services.

So, with that, thank you very much.

MS. CHRISS: Thank you, Mike, that was a terrific overview.

(Applause.)

MS. CHRISS: 240 million American wireless customers and 56 percent of them are accessing the Internet on those wireless devices, so this is certainly an important problem that touches a lot of people.

Next we have Dave. Dave, please come on up and tell us about how we can secure all of these customers.

MR. CHAMPINE: Sure, thanks. Let's see, there we are. That's me.

Good afternoon. Thanks, everybody, for sticking it out through the last session here. It seems like we've had some great discussions and a lot of consistency, that's great to hear as well because that means we can start to standardize on practices as well as policies around these issues.

Michael did a great job of kind of painting the backdrop of the wireless industry, particularly, and some of the advances there. That's one of the areas

that I will touch on in terms of my take on emerging threats.

Just two seconds, if you're not familiar with Cloudmark, we do work largely with many of the service providers in both the fixed and wireless space. We're a global business, so we do see a lot of spam, and so some of the insights will be from a consumer perspective, but some of the insights will also be from a carrier perspective, since those are our largest customers in our base.

So, a lot of the economics has been covered, and that's actually great, because we need to start thinking about this more as a business problem and less as a technology problem, if we're really going to make progress. A lot of people have already brought up the points that I have made on this slide, so this will help me kind of get through these quickly as well.

We've already identified that these are, in fact, businesses, and we talked about the different products, so I will be able to skip over my next slide pretty much specifically, but the one area is kind of market expansion, so I'll drill into that a little bit.

So, there's new technologies that they're able to exploit, new tactics that they're able to exploit, and we've heard about those and will continue to hear

about more. But one of the things that we need to understand to predict the behavior is where will they go next. If we are successful in regulating their behavior and their current tactics, where will they go next?

That's the nice thing about wireless is that it interferes with microphones.

(Laughter.)

MR. CHAMPINE: Yours will be even worse, I think. He's got an iPhone, so he's going to have a lot more interference. He's just showing off now.

In any case, if we see these like a free market, and the beauty of the Internet is that it creates a global free market, well they will move on, they will find other places to ply their wares, so let's try to predict those movements and not be caught by surprise like we have been for the last ten years.

So, we've talked, you've heard about some of the new products or tactics that these businesses are using, image spam was a big deal last year, starting to actually see somewhat of a tail-off in that in respects. It's hard to tell whether that's a trend or that's people just shifting around their tactics. Botnets are big, and Scott I think will drill into that quite a bit more and we've heard about that.

But the targeted scams, social engineering,

we've started to see a huge increase in those. Social engineering, I've heard in a number of contexts, in the session so far. What I'm referring to here is a combination of things. It's really just playing on human nature, as opposed to using specific technical capabilities. One of the things that we've seen most recently, particularly with new viruses and new outbreaks of spam with the things like the Storm Worm and different variants of that is the timing of their release.

So, in one aspect, you can use social engineering to use a compelling subject line, such as take a look at the video attached from the latest European storm. That's one context for social engineering. Another is sending out that message on a day when traditional anti-virus firms are going to be slow to respond, because they have researchers who are humans, who need to be able to take a look at that, they need to be able to reverse engineer it, in order to put out a patch.

Well, the attackers are getting more sophisticated and are saying, well, why don't I release that Saturday night just before Easter when those people will be home with their families and they won't be able to respond and I will have a window of opportunity to

infect more computers if I take advantage of that social aspect of engineering.

So, there's a number of sophistications along social engineering. We have heard about some of the terrorist aspects and ransom aspects, so I won't go into those, but I think it's interesting to point out that there are other trends along those lines.

So, let's talk about the new markets. It's not just for email anymore. Wherever you look, instant messaging, people are spamming, constantly. People are doing harvesting attacks against all of the major instant messaging providers. Comments in blogs are pretty much becoming saturated with spam, and it's pretty annoying, and there's a whole debate over whether capture is effective anymore in actually registering blog users and things like that, but you are finding spam becoming an issue in blogs and news feeds.

Social networks, I'm sure we'll hear much more about with respect to MySpace, but Web 2.0 is a concern there as well, it's another vector for people to exploit, because you're out there double clicking on stuff and that's a great way to get into your computer.

So, the big area, though, that we really ought to pay attention to is mobile, and really if you take a look at this from a macroeconomic perspective, this is

ready to burst. What we've been creating, and what CTIA has been doing a great job of creating, is an environment in North America, in the U.S. particularly is what we're concerned with here in this audience, that is ready to explode as it has in other markets. We're not used to being late technology adopters in the U.S., we're used to being a mass exporter of technology, but if you take a look at different markets around the world, particularly in Asia and Europe, where they've had these 3G networks in place for longer and there is no such thing as a smart phone in Korea, for instance, it's just a phone. It happens to be smart.

And in that region, as well, spam on those devices is incredibly high. In fact, in Korea, spam on phones is more common than spam on desktops. So it's a kind of a topsy-turvy model for us to think about. So, we do have an opportunity, and because we've got industry support and people working together, we do have an opportunity to get in front of it.

So, but let's think about it, let me drill into it just a tiny bit more. This is a very large, very grilling audience, and typically they're uneducated with respect to what the threats are, and we are kind of in a mode to borrow a phrase from another Washington person, we are in a phase of rational exuberance, with the

applications and the data services that are being deployed to mobile handsets.

Mobile advertising is expected to exceed $10 billion in the next couple of years. We don't know who's going to get all that money, exactly, but somebody is planning on spending it, and they're expecting the consumers to respond in a positive way.

There's also a lot of expectations on mobile commerce and mobile banking and mobile peer to peer payments and things like this. Well, there's a lot of high expectations that require a lot of trust and a lot of security that just isn't there. A lot of education that absolutely isn't there. So, we need to be very careful and very cautious.

Basically I'll break these down into two categories. I won't go into a lot of technical detail, just kind of spell out where these things are coming from. Michael mentioned that at the wire line to wireless convergence, fantastic technology in gateways that's starting to bridge all these. You're starting to see a lot more triple play and quad play, convergence between your online carriers offering wireless services as well.

This is great, but as he said, it opens up the walls to the walled gardens that have been protecting us

to date. There's also convergence in the handsets, convergence in the operating system which has been a barrier and provide more abuse or a wider opportunity for abuse.

So, then we have wireless-specific threats. So, spam is an obvious one, but we are not a great user of SMS here, and so we haven't experienced it all that much, although people who are heavy users, according to some surveys, 18, 20 percent have already experienced it here in the U.S. Smishing, also known as phishing, you can imagine.

The problem here, as we've talked about with phishing, a lot of it is education and being able to determine what's a legitimate link and what is not. Well, on a screen this big, you don't really have the same kind of tools or the same visibility into whether that is a legitimate link. All you have is a button that says okay. Well, if my choice is to click okay, I'm going to do that pretty often.

There are a number of exploits already on Symbian OS, which is the most popular operating systems for mobile. There are new threats all the time. iPhone creates a great opportunity as we're starting to see convergence between desktop operating systems and applications and mobile operating systems. There's a

number of threat vectors already out there.

So, what I would leave you with is what are the considerations about this, and why is this one worth particular consideration? As opposed to kind of just doing a doom and gloom scenario on this, let's think about these issues, let's address them before they become a real problem.

Young people are the primary users of mobile messaging. As I look around this audience, with all due respect, I would not expect that you are heavy SMS users. If you have children, though, I would expect that they are. If you haven't already gotten an unlimited SMS plan and you have a teenager, I highly encourage you to, because you're spending lots of money. I'm sure CTIA members appreciate that, but it's interesting. They have a nearly unlimited appetite. But that brings up a negative side. That makes youth more of a target because they are the largest segment using this, and so that's a concern that we should pay attention to.

There's a different aspect, mobile bullying is a big deal in the UK. People sending images of kids who have been beaten up. People sending threatening messages to other people. The problem is, that a lot of parents give their kids cell phones as a safety line, so

that they can always get in touch with them, so they always want them to have them, but that same safety line is being abused by their peers to bully them. I don't know what you can do about this, necessarily, but you need to take some of the same stands, but the point is that there are different issues at play than we would find in a fixed line world, and they're harder to monitor because they're so distributed.

Again, the ISPs, in this case the mobile carriers, often have more at stake as well. This can be an identification device, this can be a payment method, and the wireless carrier has a different relationship to that subscriber than an email provider does. An email provider basically is just a flow through and they bear no responsibility, they're just a channel. Whereas with the wireless carrier, they have a totally different set of regulations, they have a totally different set of expectations, and on a regular basis, they are bearing the liability for this fraud.

And as I mentioned already, it's difficult to manage this, it's difficult to deploy the right kind of tools because there are so many platforms. Fundamentally, consumers want features first and security later. So, it's being widely marketed that you have Safari on your phone, and you have OSX on your

iPhone. That is a great feature, but it's also potentially a security challenge.

So, we need to keep these in mind. It's coming our way. We have a chance to get in front of it, so thank you for your attention and on to the rest of the panel.

MS. CHRISS: Thank you, Dave.

(Applause.)

MS. CHRISS: Next we have Scott Chasin to tell us a bit more about this area, and Scott, as you make your way, Dave used a term, smishing, SMS plus phishing. I want to tell you, I read today that ginormous is now a word in the dictionary, gigantic and enormous. So, I encourage you all to use smishing, spim, spit, as often as you like, I think there's some legitimacy to that. So, let's continue. Scott, tell us your point of view on this.

MR. CHASIN: I'm just here to demo the iPhone, I think. I'm the local fan boy. So, in the interest of time, I have a presentation that I'll give you that really is regarding botnets and the evolution of botnets, that's where I spend a lot of my time these days. The CTO of MXLogic, we're managing a filtering service, we have about 18,000 businesses that we filter mail for in the cloud. Some of this presentation is a

bit technical, so if you are not an engineer, I will do my best to bring it up a level.

One interesting note, on mobile spam in Japan, I've been spending a lot of time in Japan recently. Spam is a huge issue on the mobile phones there. DoCoMo has an incredible amount of saturation of spam on their networks, and the biggest solution that the end users have found is simply to change their email address. That's partly because there's not a real good technology solution that won't impact the operator's revenue since each of the phone users actually pay per message that's inbound, right? And that's a challenge that I think that we have that spans across a lot of different devices, a lot of different markets, and I'm going to talk a lot about push and pull of how this problem is going to emanate and evolve, and impact a lot of different economic infrastructure.

So, that said, I'm going to talk about the evolution of botnets, and really I only have three slides. I know we're getting into the stretch here. I'm going to talk historically about what we've seen, on the botnet evolution, and then really where we're going, and give you some I think examples that will highlight the future.

For those of you that probably remember this, in

1988, Robert Tappan Morris created the Internet worm, which used remote scanning vulnerability checks to saturate the Internet and it spread very, very quickly. That was almost 20 years ago. Here we are today, where remote vulnerability testing is still a very valid opportunity for the propagation of worms. Not only worms, but the infection of Trojans to create botnets.

This push evolution, though, quickly, I think, scaled into the email medium, in that the social engineering aspects of email laden viruses in the associated attachments quickly, I think, became news topics and had a lot of success in the nineties, if you remember Melissa and Kournikova, and then obviously not too long ago, the Sobig and the MyDooms and we saw just this huge wave of email worms hit the net, largely being propagated by kind of the egocentric hackers.

I think that everybody's in agreement here that times have changed, we have now moved away from the ego-driven motivations of those that want to create viruses to make a name for themselves, like the eighties hackers did, and now into this new world of organized crime and financial motivation.

But that's always, I think, impacted the evolution of how these technologies are developed and deployed. So, we've seen email with social engineering

wrapped around attachments which were malicious, we are now seeing email obviously that have social engineered URLs, click on this link and then something malicious happens to you, if you do.

We have seen within the last couple of years the push mechanic of simply sending out an email that takes advantage of some kind of exploit, let's say, in your mail client, which then infects your machine, simply just by viewing the email message. And then we've also seen the automatic execution of attachments that are embedded in messages.

Now we're seeing, quite common, other exploits that are being taken advantage of in common attachments, right? So, whether you're talking about office documents PDFs, these are things that are being targeted. But I would say that the push method, which has largely been a random shotgun opportunity for the hackers, is slowly going to decline in its favor, and make way for the pull evolution. That's a random, rogue bullet point that's infiltrated my presentation. But the move to pool I think really represents a reaction to what the industry has done over the last few years, and that is we've created inbound filtering barriers.

So whether you're talking about inbound content filtering or home firewalls or other inbound security

solutions, we've started to derive in essence the threat vector to a pool mechanic. What that means is that we're seeing often times the threat come down off of an end user click off of a download where you have some kind of bundled malicious application that's co-existing with some kind of Trojan carrot, screensaver, I think, application was mentioned earlier.

You have even bigger of a threat, the web injection techniques that are being used, taking advantage of browser exports, leveraging I-frames, Javascript, and then within that, I think you have what quite could be the big sleeping giant here, which is the cross-site scripting, cross-site scripting forgery issues, which are just now coming to light really over the last couple of years and I think will have an enormous impact on the Web 2.0 infrastructure in industry, and I will talk more about that, hopefully with the panel as well.

So, this push versus pull evolution is interesting when you start to really look at the technology. What's driving botnets really, which is going to be the command and control channels, and we're seeing this evolve very rapidly. I mean, we've come a long way from IRC command and control. It's still, however, a low-hanging fruit for what we would call the

script bots out there, bots that you simply download and install, creating your own little botnet or using IRC channels to communicate. But these things are easy to detect.

One of my roles is the chairman of the botnet subcommittee at MAAWG and so we get to explore a lot of the different methodologies of detection models, and obviously the low-hanging fruit here is to be able to detect outbound IRC packets, essentially command and control packets for these bots which are infecting these very large pools of consumers inside of an ISP's network. That's pretty easy to do. What's difficult is when they start using peer-to-peer technology. Or what's difficult is when they start using encryption.

So, encryption is a very powerful weapon when it comes to how the facilitators of these botnets are controlling each of infected peers. It means that we can't do deep packet inspection. It means that we can't use puristics within the network layer to look for certain characteristics or behavior which might allow us to tell whether this machine was infected or not.

So, in a lot of ways, the use of encryption is going to spoil a lot of detection capabilities that we know today.

So, when I look out to the future, I see two

things, with bot command and control, again which is a very powerful thing from a detection perspective that we have to understand. One is the use of encryption and the second is the use of peer-to-peer networks, where essentially there is no single facilitator. Each of the infected machines in the network itself has the ability to pass along command or control instructions to each of its peers. Thus, in fact, if you cut the head off the snake, it still lives.

And so this is a very difficult thing on the detection side. The other aspect of that is that we are starting to see more and more advancement in the stealth capabilities of the bot infection, we're starting to see the use of basically embedding any kind of command control packets in high volume common transactions, HDTP, from IRC HDTP, I mean, it's only a matter of time before things like TCP knocking and other types of arbitrary data that's passed through traditional heavily used protocols will also hamper detection efforts, putting us again behind from a technology perspective in understanding who's infected and exactly how that infection is occurring.

And then we have now the Web 2.0 cross-site scripting. So, you have these criminal organizations, which are building these botnets and facilitating them,

going out and doing whatever they can to hijack public websites. Either because of web server insecurities, because the website is misconfigured, because the website allows for user contributed content to somehow allow the attacker to manipulate those configurations, or because of some other affiliate that is injecting a banner ad that has Javascript I-Frame embedded into that site where it's passed from four different sites and is presented to a trusted website.

So, these are very serious issues in the pool mechanic as the facilitators are quickly learning that by placing malicious code on a compromised website, they could now very easily test different forms of malicious Javascript or browser vulnerabilities very easily without that shotgun random approach of the push mechanic.

The Web 2.0 cross-site scripting issues are very real, in that it really comes down to stakeless authenticated sessions, allowing an attacker basically to use your own credentials, let's say you being logged into Amazon, you go to a malicious website, the attacker instructs you, or your machine to do a one-click purchase on Amazon. It just so happens that you were logged in to Amazon. That's a cross-site scripting forgery, it's a very real threat and one that could

become even more prevalent.

I know very recently as of a couple of weeks, there are some very high level community security device and commercial security devices, firewalls, whatnot, that were found to be very vulnerable to cross-site scripting attacks.

Another mechanic of the pool evolution of botnets is the use of obfuscation, and this is very challenging, again, from a researcher perspective, it's a very challenging issue in that botnets are leveraging more and more stealth, in especially the ones that hang out on hijacked web servers, they're obfuscating that Javascript code. Even more than that, they're using invasion tactics where they'll present themselves one time to an infected user, and if a researcher tries to go back to that website to see exactly what's being presented from a code perspective, it's gone.

So, they're actually becoming very smart about who they attack, and so evasion, stealth, and encryption, in more distribution of these technologies, is going to enable more infection and even more important I think the survival times, the longevity of these infections to occur at higher rates.

So, that said, some other points that I have that are not in this presentation, it's spam, spam,

spam, but it's really about bots. So, bots are the majority driver of spam today, around the world, and I see the future of bots continuing to evolve. I see lots and lots of challenges, not only on the detection side, by also on the remediation side.

So, with botnets, historically, it's all really centered around resource acquisition, right, and we saw very early botnets go out and the botmasters, the facilitators go out and try to harvest as many bots as they could to gain control of as many machines as they could in order to spam victims or in order to hijack credentials, et cetera. That's changed so much, somewhat, as we've seen lower volume, high value attacks occur, where bots are targeted towards specific institutions or specific individuals. This is also, I think, relevant to some of the newer waves of government phishing attacks that we've seen, government represented phishing attacks that we've seen, very recently over the last few months.

So, botnet resource acquisition is interesting. Today, obviously, they focus on your consumer broadband connected PC, but you could easily imagine tomorrow it will be your television, or perhaps your Apple TV box. Or perhaps your iPhone.

So, the acquisition of resources is vital for

their survival, but even more so, what they are doing, which is also testing our capabilities in the reactive detection methodologies that we have today, is that they're testing us, so for every defense or barrier that we put into place, they now benchmark us, as to our reaction time, when we release a new signature, how we distribute that signature.

So, it's very common for these facilitators to now create very polymorphic binaries for these bots and do so at a scale which can't compete with our existing resources that we have on the reactive anti-virus signature side. So, that's a key, I think, and crucial point that we have to look at for the scaleability today versus the scaleability that we have today as well as tomorrow and how that evolves.

A couple of more points and then I'll release this, the podium. Another thing that I think that you have to look at, I think this is a nice segue, is when I look at spam, and I look at spam in the context of not just email, but all the different communication mediums, it's spam or spit or whatever, it's spam. Obviously today it's email-focused, it's blog-focused common spam. It's social networking focused, but that's rapidly changing.

The definition is basically whatever the

consumer's attention span is, that's where you'll find spam. So, today, it's in your inbox, tomorrow it's in your voicemail, but also, think about virtual worlds, virtual economies, online mass multiplayer games, all of these are experiencing record amounts of fraudulent transactions and spam that's associated with these different mediums.

MS. CHRISS: Great, terrific, thanks so much, Scott.

(Applause.)

MS. CHRISS: I think a little bit later we are going to want to explore those bot theories and actually how it is affecting or could affect mobile. So, let's reserve that for the discussion period. Rick Lane, come on down. MySpace.

MR. LANE: Thank you very much. First of all I would like to thank the Federal Trade Commission for asking me here today. This is another important problem that needs to be addressed, not just from MySpace and its 182 million registered users, but the problem needs to be addressed because it's negatively affecting the user experience for all users across all social networking sites.

MySpace, as you know, is a social networking site that allows members to create unique personal

profiles online and communicate with their friends. MySpace's extraordinary success and good will is based in large part on the special experience it creates for its users. A critical part of this experience is the user's ability to access the large network of members on MySpace; however, like all large communication networks, from the telephone to the fax machine to email, there are always those who are willing to misuse the technologies to the detriment of others in order to make a profit that we've been hearing today.

MySpace is committed to making our community as safe and enjoyable as possible for all of our members. This is an ongoing process that we are constantly reviewing and updating under the leadership of our chief security officer, Hemanshu Nigam, and a world class technology and product team and a 200-plus person support organization. In fact we're looking for another lawyer and two investigators if anyone is out there looking for a job.

MS. CHRISS: No one from the FTC, not allowed.

MR. LANE: But because we believe there's no single solution to the challenges of Internet security, MySpace employs a wide variety of methods to help protect our community. Every policy we create, campaign we launch, and tool we employ, will always be part of a

larger solution.

At MySpace, we have taken a comprehensive approach, which includes both technology partnerships, legal tools and education. Some of our back end features that we have instituted at MySpace, one is Phish Lock. Phish Lock is a technology, a tool we use that will automatically lock someone's profile if we believe it's being used for phishing purposes, and in order to stop the massive amount of bulletins that can go out from one site. A user must change his password, once they realize it's locked, in order to unlock that phish lock, and gain access and to hopefully gain control of their profile.

We've improved filters and used advanced filtering technology to prevent spam. We've also eliminated the amount of emails one user can send out each day. As some of you may know, MySpace is an internal email system, it's not an email system that goes outside of the site. We've also implemented MySpace links which I think is a very interesting tool that helps us remove bad URLs across all of MySpace. What basically happens is we tag and create a URL, our own URL, so that way once we find a bad URL, we are able to delete it across the entire MySpace network.

On the front end, we have obviously the ability,

like most of the Internet service providers and others out there, to report spam at any time through a link at the bottom of the MySpace page. You can also block and flag friend requests, which is a mechanism to allow folks who are trying to gain access to your account and block them from getting on. We also block comments, a new feature in the comments section, as we heard, some of the spamming that is going on is through blogs and comments in other areas. So, this allows our users to block that as well.

MySpace meets with technology partners, like we all do, and law enforcement around the country to solicit their view points on how we can not only enhance our user security, but also support their efforts at every level. One of the more exciting areas obviously is working with Microsoft as part of its IE7 Antiphishing Referral Program. Obviously when we find someone phishing on our site and we find the URL, handing that off to Microsoft who puts it in the database and once that URL is identified, hopefully it will be blocked by others if they're trying to gain access to that URL.

MySpace has also taken a series of legal actions over the last two years to combat spam, phishing and other misuse of the MySpace site. We have filed suits

against Sanford Wallace and Scott Richter for violations of State and Federal laws, including the CAN-SPAM Act and California's anti-spam statute. In fact, over the past year, we found over ten million spam bulletins or email advertising from Richter's websites and affiliates on MySpace alone.

Assisting law enforcement in taking on criminal action against the Sammy Worm, it says Sammy Work here, but that's because I was doing it on vacation and sometimes you just don't pay attention to what you're putting on a slide show, and the operators of the MySpace plus.

One of the most notable cases that we've had, and successfully, was against theglobe.com in June 2006. One of the best things that we felt that came out of that was that the Federal Court found that theglobe.com liable for violations of MySpace's terms of service, which prohibited unsolicited electronic communications and imposed liquidated damages of $50 per email. The Court ruled that MySpace was entitled to recover $5.5 million in liquidated damages, and this was the first court ruling in the United States enforcing the liquidated damages provision such that the one that was found in MySpace's terms of service.

Educating our users is one of the most critical

issues that we all agree, I think, in this room, is necessary of trying to ensure that they are protecting themselves, as was mentioned by Michael, that as we lose control, it's going to be the empowerment of our users to help protect against unwanted spam. One of the mechanisms we use is a very popular use of Tom Anderson. Tom is your first friend on MySpace, so when you sign up for MySpace, you see Tom. In fact, for my nieces who are 17 and 18 years old, the only reason that I have any coolness at all is because I know Tom. But besides that, he's somebody when he sends out a message, people respond, people read it, and we have used that to help explain to our users about spam phishing and provide them with safety tips so that way they have the tools and knowledge to help protect themselves. That, when we send those out, that has led to members of our community telling us about phishing URLs that they're aware of so that we may be able to take the appropriate action.

When I testified in front of Congress in 2001, it seems like it's been longer than that, but 2001 on the spam legislation, I emphasized that the goal of any legislation regulating the use of commercial email must not hinder legitimate businesses from reaching out to potential clients, but must specifically target the clear abuses. I believe the CAN-SPAM Act has provided

the Federal Government and businesses with effective tools to go after those individuals; however, we may have reached a time to examine if additional legislation is needed to create an even greater deterrent for those who continue to catalog our email systems, social networking sites and in the future mobile devices with unwanted spam.

Right now it seems as though some spammers are treating fines just as a cost of doing business. One step that can be taken without additional legislation is sending more spammers to jail, not just giving them fines, but on the legislative front, some ideas that we have looked at include adding civil forfeiture to the CAN-SPAM Act and creating even more accountability for spammers who hide behind affiliates who do their dirty work from which they profit, and that was something that was mentioned earlier today during the first panel about the problems of affiliates and control thereof.

With that, I'm happy to answer any questions and thank you very much for inviting me here today.

(Applause.)

MS. CHRISS: Thank you, Rick. Well, terrific, thanks to all of the panelists. Oh, my goodness. Chris, I apologize. Talk to us, I know you have some very unique topics to address, so let's hear it.

MR. ROULAND: Thank you for not forgetting about me. Thank you for having me here.

I made a connection with the FTC at the RSA conference earlier this year in February, I had dinner with Dale Fuller, the former CEO of McAfee, one of RSA's general managers for PassMark and Chairperson Majoras, and I got to talk to her about the future of the FTC No Call List, and she was very interested when I submitted that No Call List would be completely obsolete in 24 to 36 months as we move to sifting voiceover at the infrastructure and that we have limited ability to enforce no-call measures against, say, spammers sending messages from Nigeria or Canada or Brazil or China, and subsequently came up to brief her team on that, and that's something that I would like to talk about across the panel.

What I have in my slides, however, is kind of a profile of propagation patterns we're seeing for malcode, and I thought this was important to frame where threats are going in that most of the spam threats we see today are really just payloads from infected machines and understanding how infection patterns are moving across the network, how they're changing and being optimized for maximum impact is important to understand as we come up with new strategies to defend

consumers' machines.

I got a little nervous when a couple of the other panelists started to drive into the top of this, but they fortunately didn't spend too much time on it and left me some depth to go into this. This slide is in here, one of our engineers is actually an artist as well, and came up with these icons as well. My favorite is the sequel injection hypodermic needle there, but the point I'm trying to make here is that if 79 percent of consumers already have anti-virus, why is there a problem today? And obviously there's a technology gap with the protective measures that are being used by end users today, and the propagation methods that are being executed by VXers, which is the term for the virus writers.

There is another term I heard in here today called drive by malware. That's a continuing trend. There was a study by a consumer researcher, if you do a search on drive by malware, you'll find this, and he actually took out an ad on Google, and it was a pop-up, it wasn't a pop-up ad, it was an ad on the side of the Google search bar and it said, "Is your computer virus free? Click here to get inspected," and he had over 1,200 hits in a few hours of people clicking to infect their computers.

So, I would submit that if consumers are actually asking to get infected, they may actually not have a chance, and there are some things that we need to learn from there, and technology I think remains to be a method to solve some of those problems.

I like to use this model, because it's a model of typical viral propagation, and for those of you who can't see it up here, it's basically a bell curve with a long tail. This infection pattern represents kind of what we had typically seen in viral attacks. This one has an existence of about 20 hours on it.

And what we see is the 100 percent intensity here represents the maximum infectable population of users, and there's a similar model in epidemiology, it's called the SIR model and actually maps pretty well onto computer malcode and malcode infection rates, and SIR stands for susceptibility, infection and resistance, and in the computer world, the susceptible population is the population that is using or operating on a platform that is potentially vulnerable to infection from a piece of malicious code.

The infection occurs when that malicious code then takes a foothold on those machines and the resistance or inoculation is actually applied when a sample of that malcode is transmitted to them, just as

we get resistance from disease by becoming inoculated from it or developing resistance, our computers today have to develop resistance to malcode by receiving a small sample of that malcoding, and we call those signatures, or updates from anti-virus companies.

The last slide, 79 percent of our consumers claim to use anti-virus software, so what's not working here.

One of the changes we're seeing in propagation models is that this model is not very profitable to a spammer or VXer who is operating for profit, because in this long tail, infection we're seeing users get cleaned up, they develop resistance, they receive resistance and the malcode goes away. So, this model has been gained so that operators can gain the maximum foothold during their propagation attempts, and the least amount of population can develop resistance. So, ideally, in a bad guy's shoes, you're going to infect the most mal population with no resistance being deployed.

There's obviously also a technology gap in that we are depending on a sample to be transmitted. So, that means we have to find a piece of the virus itself, transmit a tiny piece of that out to hundreds of millions of PCs.

So, we began to see a change in the patterns for

malcode propagation a few years ago and we call this first change of attack short span attacks, and it's interestingly enough working in the AV and security industry for quite a while, you may not know the fastest way to get an anti-virus company to put out an update. The fastest way to get an anti-virus company to put out an update is to have the media write about it or publish something about it. It can be the smallest, most innocuous virus or Trojan horse that only affects 100 users, the fastest way to get an update on it is for it to get profiled in the media. It doesn't matter if 100,000 users are infected, that's secondary to media coverage.

So, it's interesting, and the VXers seem to have recognized that, they want to get their malcode out under the radar, if you will, not that the media is a very effective malcode detection source, but they're simply one vector or source of potentially notification to these AV companies.

So, what they began to do was combine spam distribution methods with malcode propagation methods to get a quick shot of malcode out and then subside or stop the propagation very quickly. These two, these two characteristics generally lead to fewer notifications, fewer emergency updates, and fewer complaints from

customers, forcing AV companies to transmit out inoculation to population.

In the last two years, a more modern type of attack has emerged, and I'll expand a little bit on what Dave had talked about, and we're calling these attacks serial variance attacks. These serial variance attacks are completely gaining the inoculation model we have today in the AV industry and they're doing it to extend this window of infection.

What we actually see in software engineering, we have a term called QA testing or quality assurance testing and that's where we test or QA our products to make sure they work the way they're supposed to. We're actually beginning to see QA testing of viruses, so we're seeing computer viruses are going through rigorous software engineering technologies to make sure they function properly and most important that they are not detected by the AV products.

So, we see entire families, a family of viruses is a group of computer viruses or bots derived from a similar code base that are pre-engineered at once but signed so that the same inoculation pattern or signature pattern won't catch them and nobody can see them released on these iterative cycles and closely based intervals, again using the spam-based propagation

techniques to transmit these out, and you'll see the timing on these serial windows is designed to really tax both our ability to update our systems as well as tax the traditional AV industries method.

So, there are two examples here. One is the Storm Worm, which was mentioned earlier, another one was the WZ Stration, which is really one of the most aggressive types of these serial variant storms we've seen. So, Stration was interesting, because it almost iterated on a weekly cycle, and operated on kind of a normalized schedule.

In the first attack we saw, we saw 32 variants in ten hours. Exactly a week later we saw 61 variants in 24 hours. You can read the rest of these, again, with the Storm Worm, starting this year, we saw a maximum of 55 variants in 19 hours. Of course, if you're updating your antivirus software once a day, you're going to be 54 variants behind on this attack.

And so one of the things I think we have to do is challenge industry to invent new ways to detect and block malicious code. This does, however, lead us to some of the more interesting propagation methods we're seeing in the next generation platform, specifically around mobile devices. I was actually called out last year to a large mobile carrier in Europe, and with over

100 million users, it was an emergency and they wanted us to clean a piece of malcode off their network, and they were seeing about 5,000 infections a week. I said, well, 5,000 infections a week, you're doing pretty good with 100 million users. And they said, well, Chris, this malcode destroys cell phones, the users basically throw away their cell phone and they have to buy a new cell phone.

I said, that's kind of expensive, if you have to replace 5,000 cell phones a week, we'll get on this and fix it for you. And we found a way to detect it, but what we were seeing were variants of a phone virus called the Com Warrior Virus, and it's very interesting, there have been about 30 variants of this virus that affect mobile phones and they were experiencing with diurnal propagation method, which allows for one propagation method during the daytime and a different propagation method at night time. In this case they found the most propagation method for this virus was to actually propagate over the Bluetooth vector during the daytime so it actually turned on your Bluetooth on your phone when you're commuting to work, say on a train, infect everyone around you via Bluetooth. At night it would turn off your Bluetooth, interestingly enough to preserve battery life, and transmit to all of the people

in your phone book by SMS and the next morning would start the whole thing over again.

We actually saw a version of the worm that propagated only over Bluetooth but your battery life was limited to a few hours, what was happening is consumers were taking their phone into the store and asking for a new battery on their phone, which was expensive costs.

So, I think the last point there, to tie in voiceover and PDA, we will talk across the panel on this, we were seeing the methods applied to propagation. I think the code knows no boundaries as to platforms whether it's iPhones, Symbian, Windows Mobile, or other mobile platforms. But the last convergence we're going to see that will really sew all this together is in the next 18 months in the United States, our mobile carriers will converge voiceover IP and mobile handsets. When we get a zip stack, a voiceover IP stack on our handsets, that becomes a very attractive target, not only for transmission of spit or spam over mobile telephony, but for receiving unsolicited calls.

Today we've got dribs and drabs of voiceover by PDA users, two and a half million a year, five on Vonage, a few on Comcast, but when our carriers cut over 50 or 100 million voice users overnight, we're going to have a very target rich population in which we will

begin to see attacks against that population over this new protocol.

So, I think that was it for me, and we'll go to the panel.

MS. CHRISS: Yes, thank you so much, Chris.

(Applause.)

MS. CHRISS: So much of this information is just jaw dropping when you hear about some of these potential threats, but what I want to do is spend just two minutes honing in on exactly what are these threats? I want Scott, for example, to tell me how can my mobile phone be turned into a spam bot? Just tell me how that works.

MR. CHASIN: Well, if you have an iPhone, it can't. Spoken like a true fan, I believe. You know, it's largely going to depend on the security of the operating system. The open paths into that device, I think obviously it's been shown, Chris has mentioned that Bluetooth can be an enabler. I think there's lots of different threat vectors that exist. The problem that we have is that we want these things to become more and more advanced, which means more capabilities, and so they are resembling truly a mobile desktop, and I think that the iPhone is a really good example of a device that within its first few hours of being born was hacked over and over and over again and continues to be.

So, it's only a matter of time before we see that transmission the bridge that's built. We've seen it in spots, around the world, but I think that it's around the corner, it's not here today, simply because the bot resource acquisition is just so enamored with our consumer broadband PCs, but there's a lot of different paths in there.

MS. CHRISS: Okay, okay. That's good. Thanks so much, Scott. Now, a few of us here on this panel, we talked about how what's happening overseas is really a good way of determining what we're going to see here in a few years. I want to hear concrete examples. What's happening? Chris, you gave a good one.

MR. ROULAND: Sure. Actually, we studied malicious code from overseas quite a bit, and in certain parts of the world, we're seeing some more advanced online technologies. A great example is Latin America where PayPal type functionality is standard in all online banking.

The new malcode we see from there is particularly scary, we're calling it stakehold phishing bots. The way they work is your computer gets infected with this bot, once you've logged into the bank, it hijacks your credentials and withdraws, via their built-in PayPal functionality, money from your bank

account.

Normally it wouldn't be a big deal because you would expect to see that money missing, however it actually maintains stake or keeps track of the money you withdrew from your account and when you go to re-render or review your HTML page, it adds that balance back in, so your balance appears to be whole.

Typically for online fraud you've got 90 days in our country for an ACH, to remit a fraudulent ACH and after that it's over. So, we're seeing this very sophisticated, multi-factor authentication theft, and maintaining stake on the transaction is actually made to defraud the consumer, I think we've got a lot of exposure there as we move to those types of online services.

MS. CHRISS: Okay, terrific. Dave, you talked about how in Asia, they've been using 3G for a while. What can we expect based on what you know?

MR. CHAMPINE: Well, I mean, we see a number of exploits that, again, are jaw dropping. There's an example that I run across a few days ago called FlexiSPY that there's consumer products that are available for sale by pseudo legitimate businesses, and you can literally download this on to Symbian, BlackBerry or Windows Mobile and it is a complete espionage tool. You

can record voice conversations, you can intercept all SMS messages and emails, you can remote control the device over SMS. So, things like this already exist, and they're already serious problems. It's just that we haven't experienced them here, because we don't have the same usage profile as Europe and Asia.

MS. CHRISS: Okay. Are you seeing solutions being developed in Europe and Asia?

MR. CHAMPINE: Yeah, definitely, and some of it is coming through traditional security vendors. A lot of it is coming through a collaboration of the carriers, the handset manufacturers, and the security firms, and that's probably something that because it is a bit more of a closed loop, there's more constituents, but at least it is a bit more of a closed loop, we're seeing that more in the mobile space than we have historically in the wired space.

MS. CHRISS: Dave, you used a great word, collaboration, that's an ongoing theme for this summit, and I think that's what we'll see here in the States and in the U.S. and North America that it will be about collaboration between public and private entities, for example, global cooperation. So, that's good to highlight.

MR. CHAMPINE: And I think we have a better

opportunity, because there aren't as many national boundaries and nationalistic tendencies, hopefully.

MS. CHRISS: Yeah, yeah. Well, good. Well, Mike, I know that you work with hundreds of wireless providers and your organization can be such a good source of information. Are you guys considering whether or not to kind of get consumer feedback on their experience with malware on their cell phones? Is that something you anticipate being able to study?

MR. ALTSCHUL: We don't have the visibility as an industry association that any of our members and our large members have. But there are industry forum, or I guess we should say fora, where the subject matter experts from the industry gather regularly and share this information and we've participated and observed it.

So, it is being monitored, it's not necessarily being monitored by CTIA. Again, because it is a global industry of global platforms, we have the benefit of knowing what's going on elsewhere.

One of the earlier questions you asked is what else have we seen and what are some of the responses. A couple of years ago, I think that everyone was aware of Bluetooth's vulnerability and identity theft base. There was something that was nicknamed I guess blue snarfing, where if your phone was turned on a Bluetooth

port, malware could actually access a lot of the stored information in a device, and be exported not over the commercial spectrum, but over the Bluetooth space.

Just last month I was visiting a Bluetooth special interest group here in Washington State, and they were talking about how they have re-engineered the Bluetooth specification and interface has now released 2.1 or whatever. So, as to make Bluetooth more secure. So, it's that kind of iterative learning of vulnerabilities and engineering solutions and then releasing them that will allow us, we hope, to remain a little bit ahead, a half a step ahead of most of these threats.

MS. CHRISS: Well, terrific. Rick, we watched in amazement as you talked about the different cases that MySpace has brought against one of our very own panelists from earlier today, in fact. It sounds like the exploits are really taking advantage of technological vulnerabilities. MySpace, it's uniquely situated. You've got a community, you've got a captive audience, and these technological tools seem to be easy to use.

Can you tell me about what technological steps your guys may be using to thwart the efforts of the bad guys?

MR. LANE: We're always trying to develop new and innovative ways of protecting our users. I mean, that really is the biggest complaint we get from users of especially when somebody has hijacked their profile, and their friends think that they're sending out these bulletins on different ads for different types of products and services that are out there, and it is really hindering the user's experience.

I mean, obviously there are things that we are looking at and doing and testing that we don't talk about, because you don't want to give a roadmap to the bad guys of what we're doing, but looking at working more closely with law enforcement and the FTC and others to go after those individuals who, again, someone who is talking about social engineering I think is the term that someone used. I mean, MySpace and social networking sites are created for interaction, and they are using those vulnerabilities across Bebo, Facebook, MySpace, Xanga and the rest as a way to hijack or sell products or other malicious things. So there's an educational aspect.

As you mentioned, in talking about the technological side, I think the phishing, our stop phishing programs that we have and in other areas I think are helpful, but sometimes it's just overwhelming

and you just need to try to figure out through the entire community what can be done. I think giving more tools to our users and having them help report when things are going bad, as we were talking about earlier on the CTIA, it is going to be one of the most effective tools that we have.

MS. CHRISS: Wonderful. That's good. Getting effective tools, technological tools, that is just another theme that we're hearing throughout the day and we'll hear more about that tomorrow. So thanks for sharing that. Another thing you said, Rick, was the arrests being perhaps the greatest deterrent for these bad guys, and I just want to put a plug in for tomorrow's panel with criminal law enforcement will be here and present and telling us all about it. So, I hope everyone comes back for that.

Now let's open it up to the audience just for a few moments here. Do any of you have any questions for these panelists? It looks like I have one here. Let's take a look. Great, let's start with this one.

We've heard about financial motives earlier, what are some of the other motives that spammers have going on for them and what are some of the motives regarding these emerging threats? Is it financial also, are there other motives here for these guys in terms of

targeting mobile phones and social networking websites?

MR. ROULAND: I would say no, it's all about the money.

MS. CHRISS: All about the money, okay. Anybody care to add to that?

MR. CHASIN: I mean, there are trends that we have seen in recent news, very recent, of using, in particular botnets as weapons. So, whether that's in denial of service attack to take down or cripple the infrastructure of a government and we've seen throughout the last four years, lots of examples of that, and that's a growing trend.

We've also seen the terroristic use of botnets for dissemination of hate messaging, such as the Sober Worm and its infections. So, there are outside of economic gains, which I would say is primary today, the motivation, there are trends that can point to botnets and the delivery capabilities of them, and the destruction capabilities of them to be used for malicious purposes or to promote certain ideologies. So, they are good examples of that.

MS. CHRISS: So, not just about the money, we've got issues like terrorism, we've got some serious issues here that are at play. So, that's a good thing to raise, thank you, Scott. We have an audience member.

MS. SONIER (ph): This is in a similar vein, I mean, I don't understand the economics.

MS. CHRISS: I'm sorry to interrupt, could you state your name and affiliation.

MS. SONIER: I'm Julie Sonier [phonetic] with the FTC. I don't understand the economic incentive for a worm that destroys cell phones, I assume it's not made by the manufactured equipment or the security company. What's the economic incentive?

MS. CHRISS: Good question.

MR. ALTSCHUL: Let me answer a different thing that we have observed, which is just a variation on an old fraud and it's not very high tech, but in the U.S. we've had 900 area code numbers which end up generating a premium charge to the caller, and there are some countries in the 809 Caribbean area code that have similar numbers that look like order numbers. This has been a problem for 20 years or so from wired and wireless phones. The etiquette of wireless phones where you actually will have a call record and many people will take a look and see that they have missed a call and want to call back, has generated sort of a phishing kind of scam, where people will call and either through spoofing or whatever leave one of these numbers on the caller's phone, solely to generate revenue to one of

these sites, and drive additional revenues to the site.

MR. ROULAND: Also, so a piece of malcode that destroys a mobile phone is a bulky piece of malcode. Other things that are available have been leveraging premium SMS services or reprogramming your phone book to dial through an alternate long distance carrier. An example of a phish attack is asking you to send a text message in response to a premium service to unsubscribe you to a Spanish dating service so it keeps sending a text message to your phone to see if you want to unsubscribe to a dating service you've joined for $10. So a lot of people say, geez, I want this thing off my phone and they just pay.

MR. CHASIN: Let me add on the bright side it's not a pathogen's best interest to kill its host.

MR. CHAMPINE: I would say that some of this is related to the new frontierness of it, so a lot of it is testing the waters, how much can we do. There are instances in India, for instance, where they sent out bulk SMS messages saying that there was a virus that would actually pass from the phone to the user, and they had many, many thousands of people responding in great fear. They had SMSes that went out in Lebanon saying that you've won a new car, and they had something like 100,000 people show up at the dealerships. Just

creating that kind of chaos in itself is a tool.

MR. LANE: And also, I mean, in terms of sending out malicious code to distract, you send it over here so everyone is focusing on the right while you are doing small attacks on the left while no one is focusing because they're focused on the right, and that's a standard technique as well.

MS. CHRISS: Very good. Very good. Yes, sir?

MR. SETTLEMYER: Carl Settlemyer, Federal Trade Commission.

I just have a question that sort of anticipates what is going to be discussed tomorrow in terms of your own views with the emerging threats. What steps, nontechnological steps, do you think that agencies like the Federal Trade Commission or the Congress should mandate in terms of trying to get out ahead of this and trying to prevent some of these things from happening and what sort of suggestions would you all make in terms of maybe your top one or two things you would see as being beneficial to consumers in terms of heading off these problems and reducing the aggregate costs of the problems can entail and impose on consumers collectively over the next decade?

MR. ALTSCHUL: Certainly consumer education from as many different voices and corners as possible.

Industry, the government, everyone has an important role with emerging technologies and emerging threats.

MR. CHAMPINE: I would say along those lines, working closely with the carriers and service providers themselves, they are going through a transition time, particularly in the U.S., and so both helping to reinforce the education, helping to standardize the policies and practices, but also acknowledging that they are switching revenue streams and that you can't be too Draconian about this, it still needs to be a business venture.

MR. CHASIN: I would say it's definitely collaboration and research, more research is needed, and this is a global epidemic, it's not just in the U.S., and the threat vector is so distributed worldwide is that we can't take that perspective.

So, I'm also, in the context of just spam, there's a lot of research I think that still needs to be done around how we manage identities online. There's I think a good opportunity there. I, for one, would really appreciate just having a new sort button on my mail client that could tell me whether or not that message was human originating versus machine originating. That one little thing obviously impacts the entire eco system of identity, but nonetheless, it's

those kind of thoughts that we need to look at from a long-term research perspective, but research and collaboration.

MR. LANE: One of the things I mentioned was providing civil forfeiture. Right now you have at the Federal level in the government, you have criminal forfeiture, but the government and law enforcement can't go after everybody. They just are limited in their resources, and creating some more teeth that we have on our side to go after individuals I think would be a great deterrent, so it's not just a cost of business.

On the education side, I can't agree more that it's very important. The problem that we find, though, on the education front, is that no one listens, as we heard earlier, and it's the same problem we find on the online child safety front is that those who listen are the ones who already know and the ones who don't listen are the ones who don't know. I mean, it's a very frustrating situation, and hitting to those 30 percent or 40 percent of the folks who aren't being active on this front is the difficult part, but that's where, as someone had mentioned earlier, the vulnerabilities are, and I just don't know how to answer that one.

MR. ROULAND: There's been some really interesting work done around sovereign network borders,

and treating the 26 undersea cables that come into this country as ports of entry and having the borders, the customs and border protection agency enforce those. Just as they would secure physical ports of entry, inspect and block all this crud that's coming into our country and allow law enforcement to focus on problems inside this country and sending our own law enforcement guys to Nigeria or Egypt to take these guys down.

So, I think it's something worth exploration and consideration as to treat ingresses as ports of entry.

MS. CHRISS: Terrific. I think that is our time for today, and I just want to share with you a few of my own observations, and that is, I'm echoing the brilliance of these panelists when they talk about collaboration, when they talk about filling the technological gap, as someone put it, and this outreach, making sure people listen to what we're telling them about how to prevent problems and how to make our education efforts even better than they are, and business education, right? CTIA members. They need to know, all of these providers, they need to know how to secure their systems as they enter into the world of convergence more and more. So, I want to thank you all for highlighting those very important points for us, and I invite everyone to join us again tomorrow, bright and

early, let's hope for good weather, and thank you. Thank you all.

(Applause.)

(Whereupon, at 5:15 p.m., the workshop was adjourned.)

C E R T I F I C A T I O N O F R E P O R T E R

CASE TITLE: FTC SPAM SUMMIT: THE NEXT GENERATION OF THREATS AND SOLUTIONS
DATE: JULY 11, 2007

I HEREBY CERTIFY that the transcript contained herein is a full and accurate transcript of the notes taken by me at the hearing on the above cause before the FEDERAL TRADE COMMISSION to the best of my knowledge and belief.

DATED: 7/24/07

SALLY JO BOWLING

C E R T I F I C A T I O N O F P R O O F R E A D E R

I HEREBY CERTIFY that I proofread the transcript for accuracy in spelling, hyphenation, punctuation and format.

SARA J. VANCE